intelligence at the edge of the network
www.critical-links.com

Critical links

edgeboxx

Internet Server Appliance User's Guide, V4.0

Copyright

This manual is copyrighted by Critical Links, SA.

Disclaimer

Precautions have been taken to assure accuracy of the information written in this user's manual. Typographic or pictorial errors that are brought to our attention will be corrected in subsequent issues.

Product specifications in this manual are nominal and are provided for the convenience of our customers. They are all correct at the date of publication. Critical Links reserves the right to make product changes from time to time, without prior notification, which may change certain specifications or characteristics shown. We therefore recommend you to check for changes or updates before using for customer projects or further product developments

No material will be accepted for return unless Critical Links grants permission in writing.

The handling, installation and usage of the edgeBOX are applicable to certain environments and may be required for code compliance. Features of the device will not provide protection against abuse, misuse, improper installation or maintenance. It is important that installation, operation and maintenance are performed in accordance with instructions supplied in the manual. Electricity and electrical devices must always be treated with caution and respect.

End User License Agreement (EULA)

The edgeBOX software is distributed according to the End User License Agreement EULA included in Annex A of this User Guide. By using the software you agree to be bound by this EULA. If you do not agree to the terms and limitations of the EULA you should not use the software.

Product Support

For product technical support please visit the following web site http://www.edgebox.net or contact us at the following email address: edgebox.support@criticalsoftware.com.

CRITICAL LINKS, S.A.
PARQUE INDUSTRIAL DE TAVEIRO, LOTE 48
3045-504 COIMBRA, PORTUGAL
TEL +351 239989100,
FAX +351 239989119

CRITICAL LINKS, S.A.
POLO TECNOLÓGICO DE LISBOA, LOTE 1
ESTRADA DO PACO DO LUMIAR
1600-546 LISBOA, PORTUGAL
TEL +351 217101192,
FAX +351 217101103

CRITICAL SOFTWARE, LIMITED
111 NORTH MARKET STREET, SUITE 670
SAN JOSE, CALIFORNIA, USA, 95113
TEL +1(408)9711231
FAX +1(408)3513330

Acronyms

AD	Active Directory
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
CLI	Command Line Interface
CN	Common Name
CNAME	Canonical Name
DB	Database
DC	Domain Component
DHCP	Dynamic Host Configuration Protocol
DID	Direct Inward Dialing
DNS	Domain Name Server
DSCP	Differentiated Services Code (Control) Point
ESP	Encapsulating Security Payload
EWAN	Enterprise Wide Area Network
FTP	File Transfer Protocol
FXO	Foreign eXchange Office
FXS	Foreign eXchange Subscriber
GRE	General Routing Encapsulation
HTTP	HyperText Transfer Protocol
IAX	Inter-Asterisk eXchange
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPSEC	IP Security
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider
IVR	Interactive Voice Response
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Interchange Format
LLC	Logical Link Control
MAC	Media Access Control
MX	Mail Exchange
NAT	Network Address Translation
NS	Name Server
NTP	Network Time Protocol
OID	Object Identifier
PBX	Private Branch eXchange
PDC	Primary Domain Controller
PDF	Adobe Portable Document Format
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPPOA	Point-To-Point Over ATM
PPPOE	Point-To-Point Over Ethernet
PPTP	Point-To-Point Tunnelling Protocol
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
QOS	Quality Of Service
SIP	Session Initiation Protocol
SME	Small Medium Enterprise
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications Service
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
VC	Virtual Circuit
VCI	Virtual Channel Identifier
VOIP	Voice Over Internet Protocol
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WINS	Windows Internet Naming Service
WPA	Wi-fi Protected Access

Table of Contents

Part I Introducing edgeBOX 1

1 Powering Up the Box ... 2
2 Connecting to the network ... 2
3 Connecting to edgeBOX's console ... 4
4 Connecting to edgeBOX's serial port ... 4
5 Powering down the box ... 5

Part II Quick Start 6

1 General Layout ... 7
2 The Initial Setup Wizard ... 8
Step 1: Registered Domain ... 9
Step 2: LAN configuration ... 11
Step 3: Date/Time ... 14
Step 4: Authentication/Authorisation ... 14
Step 5: Service Configuration ... 16
Final page: Complete Configuration. ... 17

Part III Network Configuration Reference 18

1 Network Menu ... 18
Interfaces ... 18
Hostname and Domain Configuration ... 19
LAN Ethernet Configuration ... 19
EWAN Ethernet Configuration ... 20
WAN Configuration ... 20
Wireless ... 23
Basic ... 23
Wireless Status ... 24
SSID ... 24
Channel Selection ... 24
Ignore clients with broadcast SSID ... 24
Allow all clients ... 24
Advanced ... 25
Security Type ... 25
Static WEP keys ... 25
IEEE 802.1x ... 26
802.1x configuration ... 27
Encryption type ... 28
WPA ... 28
Routes ... 29
Add ... 30
Edit ... 30
Delete ... 31
2 Services Menu ... 31

© 2006 Critical Links, SA

DNS **32**
Service State 33
Domain Name 33
New 34
Edit 34
Delete 34
Hosts 35
Servers to forward to 36
Transfer Format 36
Max Transfer Time 36
Lookup Directly 36
Dynamic DNS **37**
DHCP **37**
Service State 38
Domain name 38
Ranges 38
New 39
Delete 39
MAC-IP 39
New 39
Delete 40
HTTP **40**
Service State 40
Server Name 41
Max. Access 41
User Directories 41
Virtual Hosts 41
New 41
Edit 42
Delete 42
Change Webmaster password 42
SMTP **42**
Service State 43
Global 43
Email Domain(s) 44
Webmail Domain 44
Storage 44
Max. Connections 45
Max. Message Size 45
Block Unresolvable Domains 45
SMTP Relay Support 45
Access Control 45
Ban List 46
Relay Domain List 46
Alias 46
E-Mail Aliases 47
LDAP 48
LDAP Mail Routing 49
Enable LDAP Lookups 49
Domain 49
Enable LDAP Synchronize 49
Local LDAP Root Password 50
Samba **51**
Service State 52

© 2006 Critical Links, SA

Global 52
Global 52
Wins Options 53
Shares 53
New 53
Edit 54
Homes 55
Boxes 55
USB Printers 56
Web Filtering 57
Domains 58
Words in URL 59
VoIP 59
Phones 59
New 60
Basic 60
Advanced 61
Codecs 62
Privacy 63
Edit 64
Delete 64
Incoming Calls 64
IVR Editor 65
Edit Context 65
Add Action 66
Goto Action 68
Remove Action 68
Internal 68
Add Action 69
Call Rules 69
Add Rule 70
DID Routes 71
Add Route 72
Sound Manager 73
Outbound Calls 74
Prefixes 74
LCR 75
Providers 76
Add 77
Remote Switch 78
Add 80
Enum Config 80
Authentication 81
PBX Features 82
Manage Queues 82
Add Queue 83
Agents 85
Add Agent 86
Conferences 86
Add Room 87
Parking 88
Hunt Groups 89
Add HuntGroup 90
Voicemail 91

© 2006 Critical Links, SA

Hardware 92
ISDN BRI 92
Edit Port 93
ISDN PRI 93
Edit Port 94
Analogue FXO-FXS 95
Generic 95
3 Security Menu 96
Firewall 96
Firewall 97
DMZ 99
NAT 100
Nat 100
Port Forward 101
VPN IPSec 103
Service State 104
Active Tunnels 104
VPN(s) 104
Add 104
General 105
Network/Host 105
Start on system boot 105
Tunnel Name 105
Remote Network (Network only) 105
Remote Netmask (Network only) 105
Remote Gateway (Network only) 105
Static IP (Host only) 106
Host IP (Host only) 106
Perfect Forward Secrecy 106
Key Lifetime 106
Encryption 106
Authentication 106
Services Access 106
Host 106
Local Hosts Visible to External Hosts 107
Local Hosts Denied Access to Remote LAN 108
Edit 108
Delete 108
VPN PPTP 108
Service State 109
Connected users 109
Authentication Type 109
Local Authentication 109
Remote Authentication 110
IP ranges. 110
MailScanner 111
Shares Scanner 112
Virus 112
Options 112
Mail Scanner 113
General 113
Virus 114
Spam 115

© 2006 Critical Links, SA

More Options 116
Messages 117
Actions 118
Anti-Virus Engines 119
Sophos 120
Information 121
Upload and Install 121
Update 121
McAfee 122
Information 122
Upload and Install 122
Clamav 123

Part IV Advanced Topics 124

1 User and Group Management 124

Users 125
Groups 128

2 Policies 129

Editing a Group Policy 130
Internet Access 131
Quality of Service 131
Allow Internet Access 131
Time Period 132
Incoming 132
Outgoing 133
Service Access 134
Enterprise Access 134
Quality of Service 135
Allow enterprise access 135
Time Period 135
Incoming 136
Outgoing 136
VPN Connections 137

3 Traffic Control 137

Service State 137
Upload Information 138
Maximum Uprate 138
Premium Bandwidth 138
DSCP Marking 139
Download Information 139

4 Services QoS 140

Add 140
Edit 141
Delete 141

5 System Configuration 142

Authentication 142
Remote RADIUS Server Authentication 143
Add 144
Edit 145
Delete 145
Remote LDAP Server Authentication 145

© 2006 Critical Links, SA

Accounting **146**
Date/Time **147**
Syslog **148**
Quota **148**
Backup **149**
Backup Configuration 150
Restore Configuration 150
Config **151**
Admin Options 151
SpeedTouch Firmware 152
Web Locale 152
Root Email 153
Logs 153
Landing Page 153
System Update **154**
System Update 154
Configuration 155
SNMP **157**
SNMP RO Configuration 157
SNMP Trap Configuration 158
Logoff **158**
Logoff/Restart/Shutdown 158

6 State Menu **159**

Users **159**
Network **159**
Services **160**
Traffic Control **161**
Accumulated History **162**
Accumulated Session **162**
Session Details **162**

7 The CLI **163**

Part V Using edgeBOX 165

1 Login window **165**

2 User Data Management **165**

General **166**
Name 166
Password and Confirm 166
Activate mail forward 166
Your disk quotas 167
Activate vacation mail response 167
VoIP **167**
Settings 167
Inbox 167

3 Web Mail **168**

Part VI Configuration Examples 170

1 Scenario 1: SME branch office **170**

Step 1: WAN connection **171**
Step 2: LAN connection and security **171**
Step 3: Wireless connection **173**

© 2006 Critical Links, SA

Step 4: Services and users' accounts ... 173
Step 5: Remote users' connection ... 175
Step 6: VoIP features ... 175
2 Scenario 2: SME HQ ... 177
Step 1: Wan connection ... 177
Step 2: LAN connection and Security ... 178
Step 3: Authentication and Security ... 179
Step 4: Users and Group Policies ... 180
Step 5: Services ... 181
Step 6: Backups ... 182
Step 7: VoIP features ... 182
3 IVR configuration ... 184
4 IPsec VPN ... 186
5 Remote Switch ... 187
Part VII Services 189
1 Main Menu ... 189
2 Public Safes ... 189
3 EWAN Certificate ... 189
Part VIII Reporting 190
1 System Usage ... 190
CPU ... 190
Load ... 190
Memory ... 190
Network Received (bytes) ... 190
Network Transmitted (bytes) ... 191
Network Received (packets) ... 191
Network Transmitted (packets) ... 191
2 Web Server ... 191
Status ... 191
Request ... 192
Host ... 192
Agent ... 192
3 Proxy Server ... 192
Methods ... 192
Top Level Destinations ... 193
Second Level Destinations ... 194
Content Type ... 195
Extensions ... 196
TCP Time ... 197
Incoming TCP ... 198
Response Code ... 199
Size Distribution ... 200
4 Firewall ... 201
Firewall ... 201
Chains Matching ... 202
By Interface (Packets) ... 203
By Interface (Occurrences) ... 204

© 2006 Critical Links, SA

By Protocol (Packets) 205
By Protocol (Occurrences) 206
By Source Port (Packets) 207
By Source Port (Occurrences) 208
By Destination Port (Packets) 209
By Destination Port (Occurrences) 210
By Source Address (Packets) 211
By Source Address (Occurrences) 212
By Destination Address (Packets) 213
By Destination Address (Occurrences) 214
By Service (Packets) 215
By Service (Occurrences) 216

5 Syslog 217

6 VoIP 218

Top Callers 218
Top Sources 219
Top Destination Context 220
Top Minutes 221
Top Accounts 221

7 Anti-Virus 221

Viruses Found 221
Infections Ratio 221

Part IX Appendix A: Authentication 223

1 Authentication architecture 223

2 Require users to login vs Group Policies 223

3 Putting all together 224

4 Remote configuration 224

Part X Appendix B: VPN Setup 226

1 IPsec VPNs 226

SSH Sentinel 228
GreenBow 232

2 PPTP VPNs 234

New connection wizard 235
Editing the PPTP connection properties 237
Connecting to edgeBOX 238

Part XI Appendix C: Connecting to Wireless 239

1 802.1x 239

2 WPA 242

Part XII Appendix D: Using Samba 244

1 edgeBOX as a PDC 244

2 Public safes 246

Part XIII Appendix E: Virtual Hosts 250

© 2006 Critical Links, SA

Part XIV Appendix F: Softphone configuration 251

1 X-Lite 252
2 Idefisk 254
3 Express Talk 255

Part XV END USER LICENSE AGREEMENT (EULA) 257

Part XVI Licence texts 262

Index 0

© 2006 Critical Links, SA

1 Introducing edgeBOX

edgeBOX is an Internet server appliance suitable for many different types of network installations. From a simple home based office Internet presence to a fully featured SME Internet gateway with user-access control, accounting and Active Directory authentication, edgeBOX provides a large and rich set of communication services. Flexibility and simplicity are key features of edgeBOX and an integrated Control Centre makes configuration and administration tasks easy to perform.

edgeBOX is designed as a gateway, connecting a local area network to the Internet. A second Ethernet interface also allows edgeBOX to be connected to an enterprise-wide private network.

Main features:

- Network connections using ADSL or Cable modems;
- Optional internal ADSL modem;
- Supports both dynamic and static addresses allowing the configuration of a registered domain name if available;
- DHCP server on the Intranet side with optional automatic name range generation;
- Web server presence on both the Internet and Intranet side. Optional users home pages;
- DNS Domain name server for both local private domain or as a master name server on the Internet;
- Internet Mail server with anti spam control and LDAP based mail routing. This service is available if you have a registered domain and static IP address on the Internet side;
- Supports SMTP relay for Road Warriors;
- Full access control for both internal services and Internet access;
- User based access control. Control access to resources based on the username;
- Group based access control;
- See who is on your network and from what IP address;
- User time and traffic based accounting. Supports optional Radius session servers;
- Supports three types of user authentication, Local, Radius and LDAP;
- Configuration and User data backup and restore;
- System updates from a remote server. Keeps your system updated with the latest security patches;
- Dynamic DNS. Supports both the DynDNS and No-IP services;
- Optional Wireless Access Point feature;
- IMAP and POP3 servers. Integrated mail access using the internal web server;
- VPN gateway based on both the IPSEC standard and PPTP protocol;
- Traffic control in both Inbound and outbound. Possibility of getting a share of the available bandwidth reserved for important users in your company or for high priority traffic types such as voice;
- Support for a dynamic Intranet with content management capabilities;

© 2006 Critical Links, SA

When you open your edgeBOX package you should find the following items:

- edgeBOX;
- Power supply unit and cable;
- PS2/USB keyboard adaptor (depending on version) ;
- Installation & configuration guide;

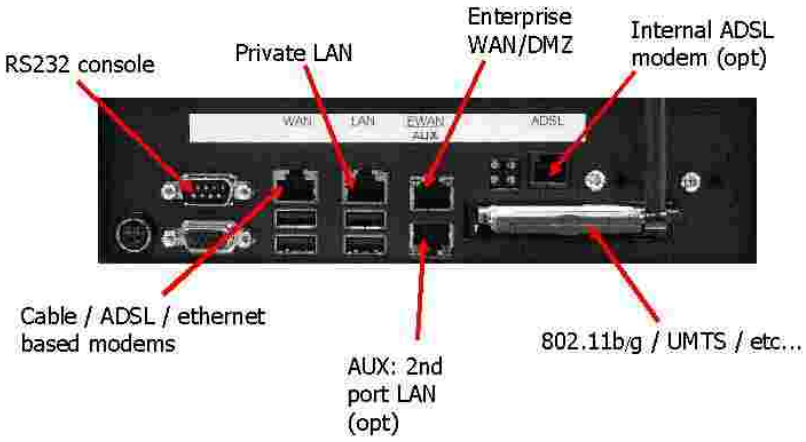
1.1 Powering Up the Box

To connect the appliance to the main power source, follow the directions described below:

- Connect the AC adaptor to the power socket located on edgeBOX's rear panel using the power cable;
- Connect the power adaptor to an electrical outlet;
- To switch on the appliance, press the button located on the front panel. A blue light will then be visible, indicating the box is properly powered.

1.2 Connecting to the network

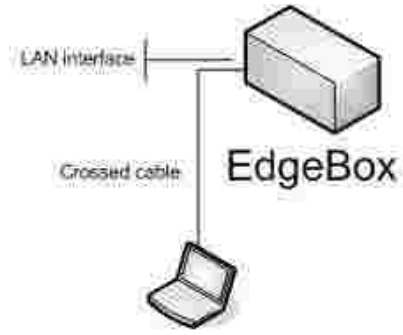
The next step will be to physically connect the appliance to the network. Although it can be used in several different topologies, edgeBOX is preloaded with a default factory configuration.



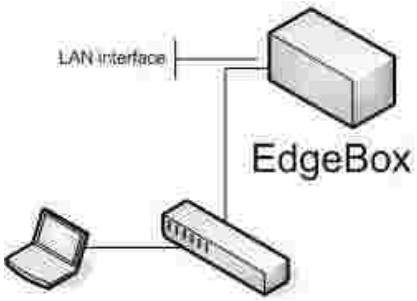
edgeBOX's Twister Model rear panel

Typically, the first task will be to change this configuration, so it meets your own requirements. The user is advised to perform the initial configuration from a PC connected either directly to edgeBOX's LAN interface, or to a device (a hub or a switch) connected to this interface.

© 2006 Critical Links, SA



Connecting with a crossed cable



Connecting through a hub

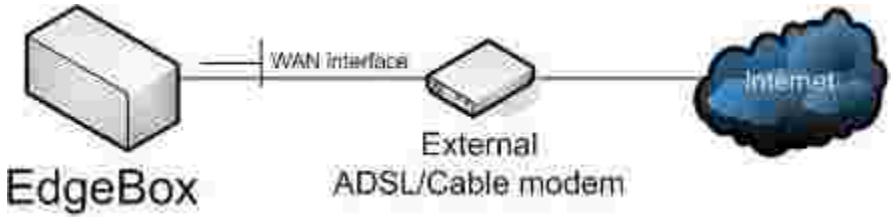
If you connect your PC directly to the LAN interface, bear in mind that you will need a crossed network cable. If you connect a hub or a switch to edgeBOX's LAN interface, then you may use a standard network cable. The interface is initially configured with the IP address 192.168.100.254 and has the DHCP service active. In order to connect to edgeBOX a client PC may be configured in one of two ways:

- Using DHCP, and obtaining its TCP/IP address from edgeBOX;
- Using a static IP address. The IP used has to be within the range 192.168.100.0/24.

To perform the initial configuration, the easiest (and preferred) way is to use the web interface. You can use any web browser, provided the java plug-in is installed. To connect to the web interface, point your browser to http://192.168.100.254:8010 (you can also use https://192.168.100.254:8011). For a detailed explanation of the steps required to configure edgeBOX, please see Network Configuration Reference.

After the initial configuration is performed, the LAN will most likely be connected to a switch or hub connected to an internal network. The interface used to connect to the Internet will depend on the method used:

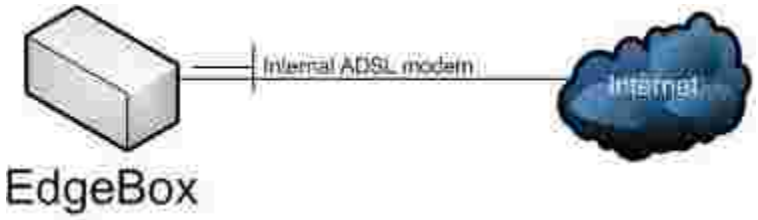
If another LAN or an external Cable or ADSL modem is to be used, then the interface to use will be the WAN interface. This is an Ethernet port located on the leftmost part of the rear panel.



© 2006 Critical Links, SA

Connecting to an external ADSL/cable modem

If the internal ADSL modem is to be used, then you will just have to plug a telephone cable from the wall jack providing the ADSL service to the ADSL port located in the rear panel.



Connecting to the Internet using the internal ADSL modem

If you want to use a supported USB ADSL modem, then you may use any of the USB ports located on the rear panel. Before setting up ADSL, make sure that your modem is correctly powered up and connected to edgeBOX.

1.3 Connecting to edgeBOX's console

It is also possible to connect directly to the console which provides a command line interface (CLI). This method provides a limited subset of commands and is recommended only for advanced users.

To connect to edgeBOX's console:

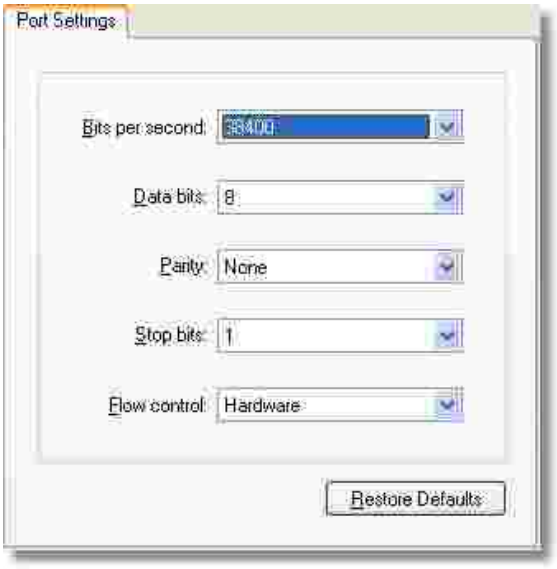
- Connect a keyboard to any of the USB ports located on the rear panel (you may use the supplied USB/PS 2 converter supplied);
- Connect a monitor to the monitor port located in the rear panel;
- The screen should display a prompt requesting a login/password to be entered.

1.4 Connecting to edgeBOX's serial port

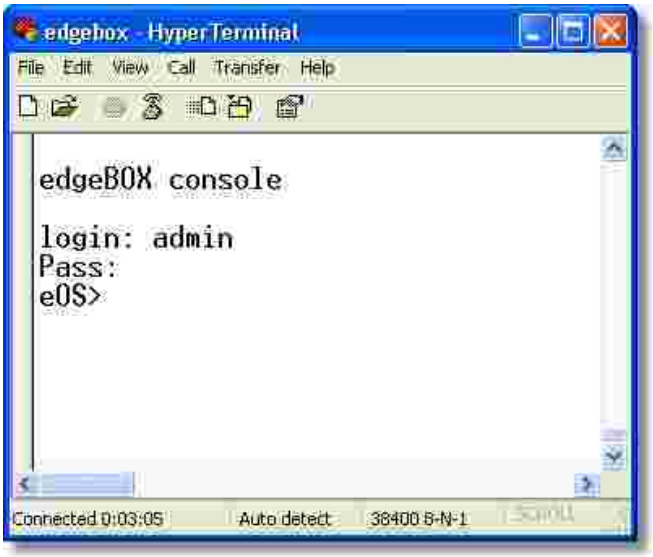
Yet another way to access the CLI is to connect to edgeBOX's serial port. You may use a terminal program like HyperTerminal. Configuration should be as follows:

- Bit per second: 38400;
- Data bits: 8;
- Parity: None;
- Stop bits: 1;
- Flow Control: Hardware.

© 2006 Critical Links, SA



Configuring a new connection using HyperTerminal



accessing edgeBOX console via the serial port using HyperTerminal

1.5 Powering down the box

To switch off the box, press the front panel button. The system will perform a shutdown and will power off. The shutdown command may also be issued either from the web interface or from the command line. For more information on shutting down edgeBOX, please see Logoff.

© 2006 Critical Links, SA

2 Quick Start

How to quickly install and configure edgeBOX

In this chapter, you'll learn how to quickly configure edgeBOX using the web interface. For details on how to connect to edgeBOX's web interface see Connecting to the network.

Initial page

Login Page

After pointing your web browser to the web interface URL, you will be presented with a page similar to the figure above. Here, you will be able to select between the administration page, the reporting page and the services page (for more information on these features, please see Reporting and Services). After following the Administration link, you will be presented with the login page. To log in, type username admin, password root. This is the default password for the administration account. The user is advised to change this password as soon as possible. For instructions on changing the administration password see Change Password.

© 2006 Critical Links, SA

General Information Page

After logging in your browser will start the Java-based Control Centre. After the web interface loads the page in the above figure will appear. This is a general information panel where you can check certain aspects of edgeBOX's configuration as well as information about the machine status (machine load, memory usage, disk usage, uptime, etc).

2.1 General Layout

In the general information panel you can see some elements common to all pages:

The header menu bar has the following options: System, Network, Services, Security, QoS, Policies, State, Users, Wizards and Help. Each of these menus and its submenus will be covered in detail in the next chapter.

The main panel is divided into two sections:

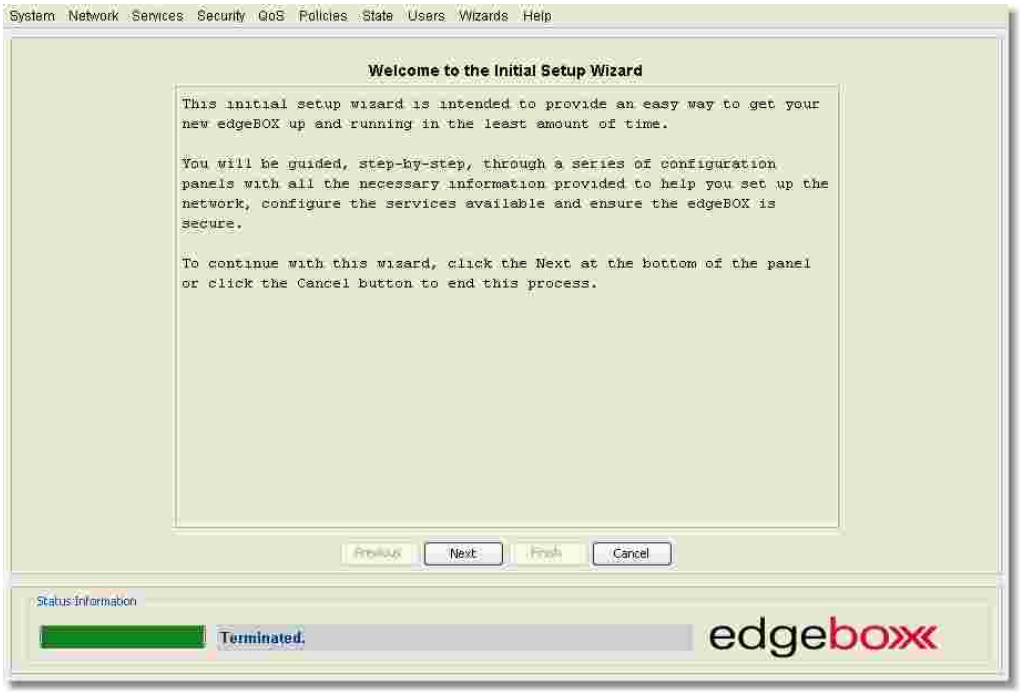
- The upper section is the working area where information regarding the option chosen in the menu will be displayed. It is also the place where configuration details will be entered;
- The lower section is the Status Information panel. It displays status information on the operation being performed. While an operation is taking place, a moving bar is displayed; once the operation is completed a green colour will indicate the operation has been completed successfully or, in case of failure, the bar will be coloured red.

Note: if you were already acquainted with edgeBOX's control centre graphical interface, you will notice that the log and the help panels have been dropped in this version leaving more space in the main panel. This manual is now available online through the "User Manual" option, in the Help menu.

© 2006 Critical Links, SA

Now we will show how to use the network configuration wizard to quickly configure edgeBOX. This is the preferred method for configuring edgeBOX if you are not a networking expert as it will lead you through each step dealing with only the basic elements. Network administrators or users with a good knowledge of computer networking may consult the reference chapters to see how the different features and services are configured.

2.2 The Initial Setup Wizard


System Network Services Security QoS Policies State Users Wizards Help
Welcome to the Initial Setup Wizard
This initial setup wizard is intended to provide an easy way to get your new edgeBOX up and running in the least amount of time.
You will be guided, step-by-step, through a series of configuration panels with all the necessary information provided to help you set up the network, configure the services available and ensure the edgeBOX is secure.
To continue with this wizard, click the Next at the bottom of the panel or click the Cancel button to end this process.
Previous
Next
Finish
Cancel
Status Information
Terminated.
edgeboxx

Wizard Welcome Page

To start the configuration wizard, select Initial Setup from the Wizards menu. The welcome page shown will appear. Pressing “Next” will lead you to step 1. If you plan to use a supported USB ADSL modem, make sure it is properly powered up and connected to edgeBOX before booting the box or it will not be detected.

© 2006 Critical Links, SA

2.2.1 Step 1: Registered Domain

Step 1(Registered Domain)

In Step 1 you will be required to enter information describing your Internet connection and domain. If you have a registered domain, then you should check “Registered Domain”. The following options will then be displayed:

- Hostname, i.e. the name edgeBOX will be known by in this domain;
- Public Domain, the name of the registered domain;
- Secondary Name Server IP, the IP address of a secondary name server for your domain, if it exists and
- Local Mailbox Storage.

Having a registered domain inactivates the check box “Obtain IP automatically” - the addressing scheme has to be static. You may, however, have a dynamic addressing scheme and use a Dynamic DNS service (for more information, see Dynamic DNS). If you don't have a registered domain or plan to use a Dynamic DNS service, leave this option unchecked.

© 2006 Critical Links, SA

Options for Registered Domain

If you don't have a registered domain, you may still choose between a static or dynamic addressing scheme by checking or unchecking “Obtain IP automatically”. If you don't check this option, you will be required to enter the following information:

- IP, i.e. the IP address for the WAN interface;
- Netmask, the netmask to be used on the WAN interface;
- Gateway, or the gateway which will route traffic to and from the Internet and
- Primary and Secondary DNS: The IP addresses for your Name servers.
- If you check “Query DNS”, the DNS configuration will be fetched during connection setup (checking this option will deactivate the DNS controls).

If you check this option, then all this information will be fetched automatically from a DHCP server. When in doubt, check this option.

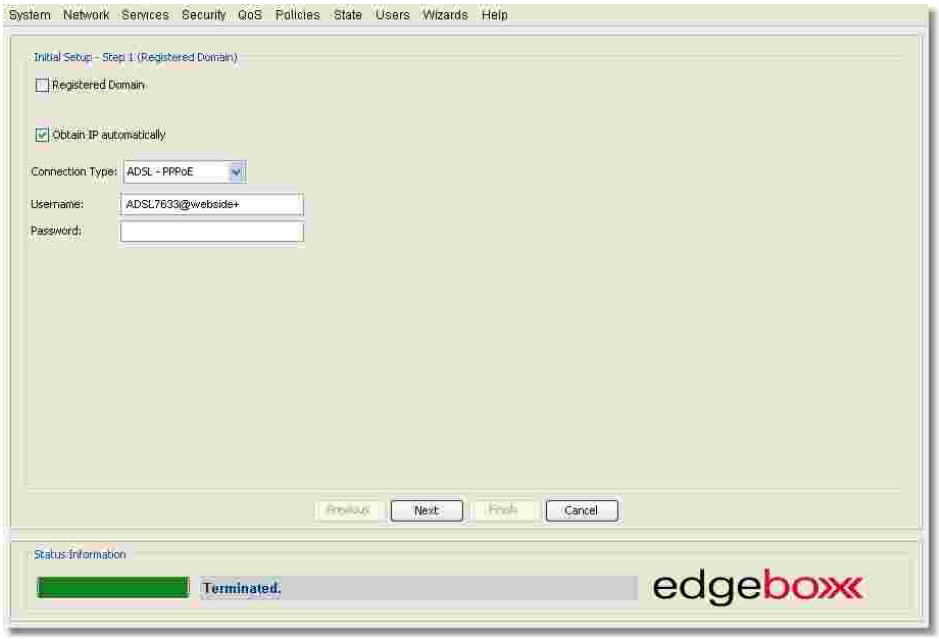
The last option will be to choose the connection type. There are two available choices:

- Cable/LAN, if you plan to connect your WAN interface to an external cable modem or to a local area network, or
- ADSL.

In the first case, you will always use the WAN Ethernet port located on edgeBOX's rear panel. Either case will be transparent to you. However for ADSL, depending on you box configuration, you may have two options: PPPoE and PPPoA. No matter which setup you choose you will always have to provide information of the username/password for your ISP account. In addition, if you choose

© 2006 Critical Links, SA

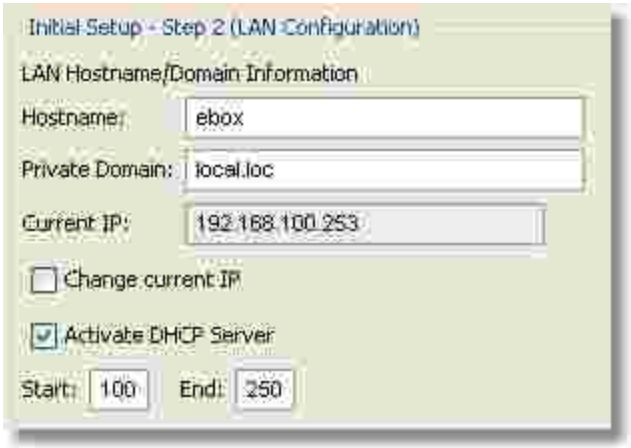
PPPoE and internal modem or PPPoA, you will have to provide the VPI, VCI and encapsulation information (choose from the list of possible values: LLC or VC). Ask your ISP for this information if you don't have it.



ADSL information (internal modem not available)

After entering all the above information press “Next” to proceed to step 2.

2.2.2 Step 2: LAN configuration

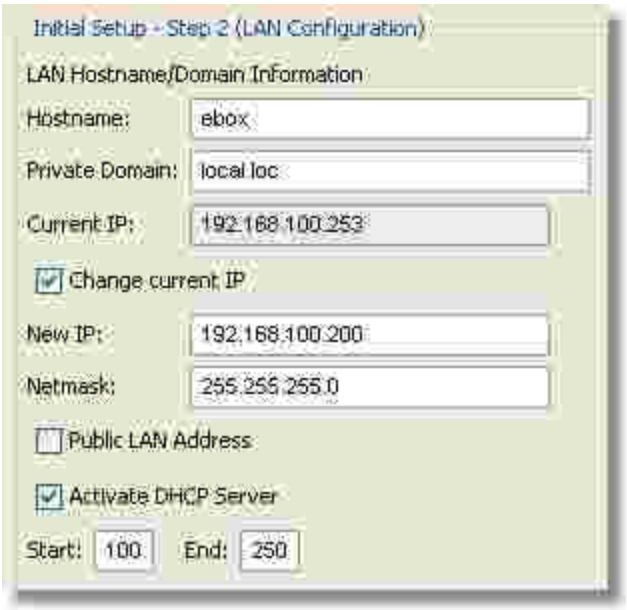


Step 2: LAN configuration

In this panel you will be required to configure some aspects relating to the internal network. In “LAN Configuration/Domain Information”, you may enter/change the following information:

© 2006 Critical Links, SA

- Hostname: edgeBOX's name in the internal domain;
- Private Domain: This will be the name of the internal domain, i.e. the domain to use in the LAN;
- Change Current IP. Checking this option will allow you to change edgeBOX's internal IP which is set to 192.168.100.254 in the default configuration. If you check this option you will be required to enter:
    - New IP: the new address for this interface and
    - Netmask: the netmask for this interface.
    - Public LAN Address. If you check this option then you will only be using valid IP addresses. If you don't use this option, your internal network addresses will be private and an address-translation scheme will be used (NAT). If in doubt, leave unchecked.



Options for Change Current IP

- Activate DHCP Server. This option is unchecked by default. If you check this option the machines on your network will be able to use a dynamic addressing scheme, i.e. fetching the IP address from edgeBOX. You will be required to enter the range of addresses that may be assigned by DHCP (Start address/End Address).

Activate DHCP Server

- Activate Wireless Access Point: This option is unchecked by default. If you check it, you will activate the edgeBOX AP, and you will be required to enter the following information:
    - SSID: the network public name. The default SSID is “edgebox” and
    - Activate Encryption. If you check this option, you will need to choose the security

© 2006 Critical Links, SA

type. Available types are:

- WEP: you will need to provide one key to use;
- 802.1x:you will need to choose the encryption type to be used, between WEP and WPA. In the later case, you will further need to provide either a passphrase or a PSK.
- WPA: you will need to provide a passphrase or a PSK.

Wireless and EWAN Options

- EWAN Information. If this option is present, you are required to enter the configuration for the enterprise interface, specifically:
  - IP Address (the default value for this interface is 192.168.200.254);
  - Netmask: The netmask to apply for this interface.

Pressing “Next” will lead you to Step 3.

© 2006 Critical Links, SA

2.2.3 Step 3: Date/Time

Step 3: Date and Time

In this step, you will be prompted to set the machine clock. The controls are initially disabled so to change these settings you have to press “Change”. The following information may be altered:

- Date (Use the up/down controls or edit directly the desired value);
- Time zone (Choose from the values present in the list);
- Time (Use the up/down controls or enter the desired value).

Pressing “Next” will lead you to Step 4.

2.2.4 Step 4: Authentication/Authorisation

Step 4: Authentication/Authorisation

In this step, you will be required to enter information regarding user access and traffic logging. The following information may be entered:

- User authorisation. If you choose “on”, access to services/resources will be dependent on user authentication (the user has to enter their username/password). Typically a profile is configured for a group of users, which will then share a particular configuration for accessing services/resources. When in doubt choose “off”.

- Authentication. Choose the method for authenticating users from the list. Available methods are:

© 2006 Critical Links, SA

- Local Server (local accounts are used);
- Remote LDAP Server
- Radius Remote Server.

When in doubt choose Local (which is the default).

Options for remote LDAP authentication

Options for remote RADIUS authentication

- Traffic Log. Choose between the available values: Off, 15 minutes, 30 minutes and 60

© 2006 Critical Links, SA

minutes. This will set the interval between traffic logs. If user authorisation is set to “off” you may also leave this setting “off”.

Pressing “Next” will take you to Step 5 (which is the final step in this setup).

2.2.5 Step 5: Service Configuration

Step 5: Service Configuration

In this step you will be required to configure access to the services running on the box. You may grant access to the internal network (LAN), external network (WAN) and the enterprise network (EWAN).

The following services may be configured:

- DNS (Domain Name Server: Used to lookup domain data);
- SMTP (Simple Mail Transfer Protocol: Used for email);
- LDAP (Lightweight Directory Access Protocol: Used to access directory services);
- SSH (Used to connect to a remote shell under a secure channel);
- IMAP (Internet Message Access Protocol: Used to access mailboxes);
- VOIP (Voice Over Internet Protocol, Used by edgeBOX's PBX);
- SNMP (Simple Network Management Protocol);
- FTP (File Transfer Protocol: Used to update the users' personal page and intranet server);
- HTTP (Used to communicate with the web server);

© 2006 Critical Links, SA

- POP3 (Post Office Protocol: Used to access mailboxes).
- CTI (Computer Telephony Integration: Used to access edgeBOX's PBX text management console);
- SAMBA (Open source implementation of Microsoft's SMB protocol);

To grant access to a service in a specific interface just check the box in the cell corresponding to the intersection of the service line with the interface column. When in doubt the user is advised to leave unchecked at least the services in the external (WAN) interface.

The user may also check “Web Server Configuration”, which will allow him to enter:

- Default Name for intranet Server: The default name to access the intranet server;
- Allow user directories: If this option is checked, each user will be allowed to have a personal web page.

Pressing Enter will lead you to the final page.

2.2.6 Final page: Complete Configuration.

In this page you are given the opportunity to review all information entered in the previous steps. This is the final opportunity to confirm all the data entered before applying the edgeBOX configuration. The options available are:

- Previous: Returns to the previous step. Since this option is also available in each step, we can in fact perform a correction on any data entered in the previous steps;
- Cancel: Aborts the configuration. All data is lost and the configuration is not applied. This option is also available in each step.
- Finish: The configuration is applied to the box.

After selecting “Finish” please be patient as this operation may take some time to execute. One of two situations may occur:

- You kept the internal interface (LAN) IP address. After the process is completed, you will return to the general information page (the first page you saw after you successfully logged in to the box) where you can run a quick check on the box configuration or
- You changed the internal interface (LAN) IP address. You will loose the connection with the web interface. Depending on your client PC configuration you may have to change its settings. Please wait some time (5 minutes) and reconnect to the web interface, pointing your browser to the new internal address of edgeBOX, port 8010 (or 8011). For example, if the new address given to the LAN interface was 10.1.1.254, you should point your browser to http://10.1.1.254:8010 (or http://10.1.1.254:8011).

© 2006 Critical Links, SA

3 Network Configuration Reference

In the previous chapter we've seen how to quickly upload a working configuration to edgeBOX using the setup wizard. In this chapter the web interface pages used to configure network options will be fully covered, allowing us to fine-tune the setup.

This chapter is intended as a reference for network administrators and experienced networking users.

3.1 Network Menu

This menu option allows you to review and configure the network settings, specifically:

- Connectivity (interfaces, hostname and domain information);
- edgeBOX's Wireless access point (if available) and
- Static Routes.

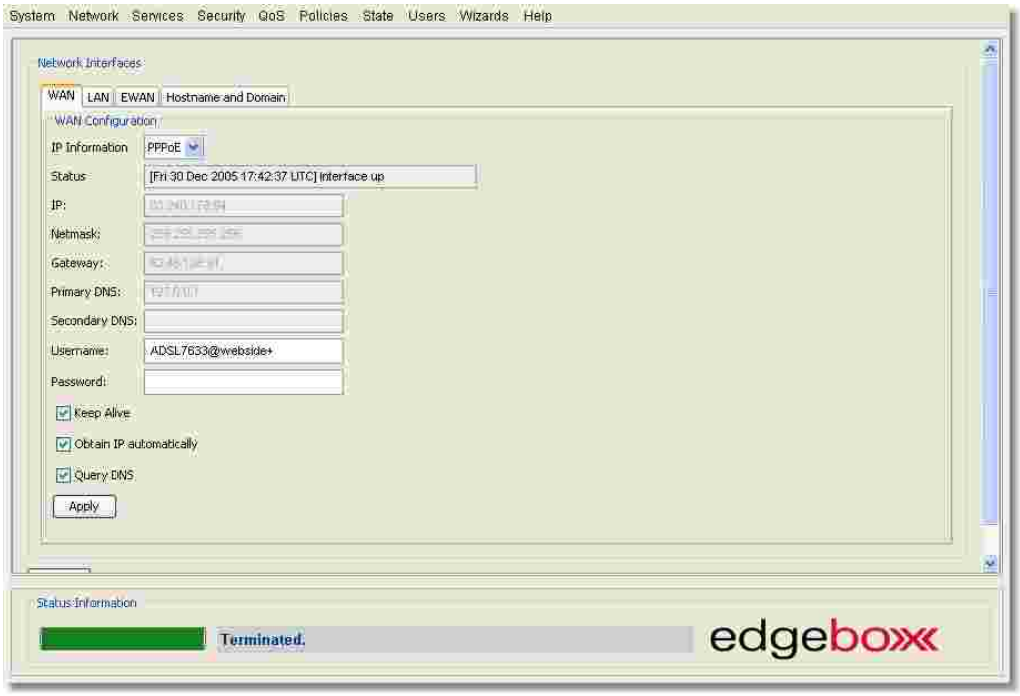
3.1.1 Interfaces

This menu option allows you to review and change the following settings:

- Hostname and Domain Information;
- LAN Ethernet Configuration;
- EWAN Ethernet Configuration and
- WAN Ethernet Configuration.

To access each of these options, select the appropriate tab.

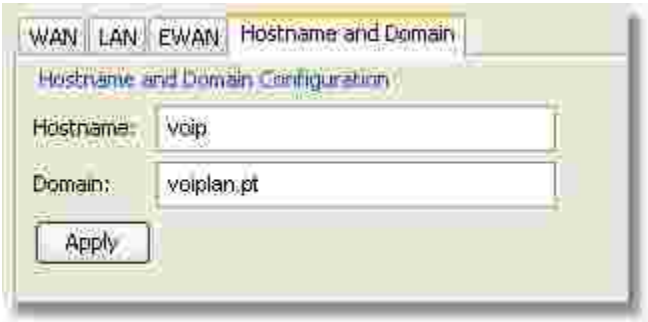
© 2006 Critical Links, SA



3.1.1.1 Hostname and Domain Configuration

To change the hostname and/or the domain configuration, follow these steps:

1. Change the desired setting(s) (Hostname and/or Domain);
2. Select “Apply”;
3. Check the status returned to see if the operation was successful.

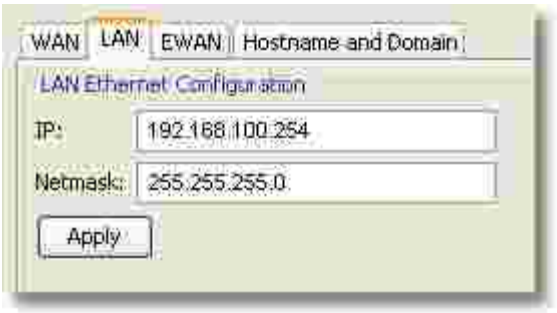


3.1.1.2 LAN Ethernet Configuration

To change the configuration for the internal interface, take the following steps:

1. Change the desired setting(s) (IP Address and/or Netmask);
2. Select “Apply”;
3. Check the status returned to see if the operation was successful.

© 2006 Critical Links, SA



3.1.1.3 EWAN Ethernet Configuration

This allows you to change the IP Address and/or the netmask for the enterprise interface. The steps are the same as in “LAN Ethernet Configuration”.

3.1.1.4 WAN Configuration

This option allows you to change the configuration for the external Interface. The information required will depend on the value chosen for “IP Information”. Available values are: Static, DHCP, PPPoE, PPPoA, UMTS or none.

If you have a cellular gateway card installed UMTS will also be available in the IP Information pull-down menu.

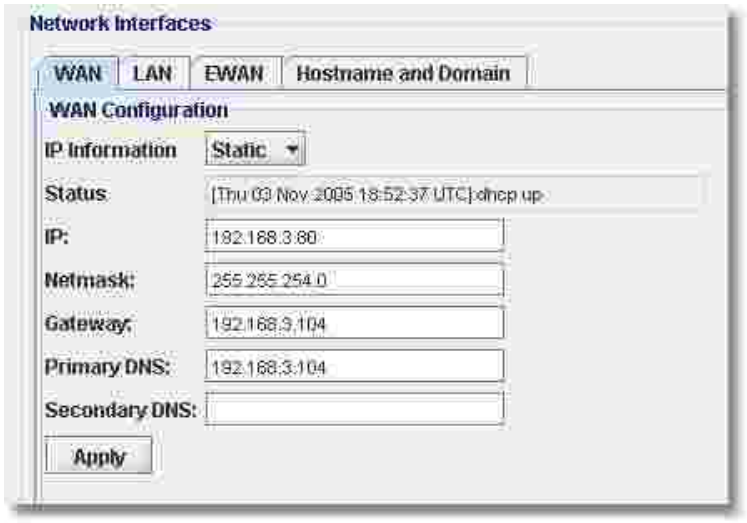
Static

If the value chosen for “IP Information” was static, the following information has to be entered:

- IP;
- Netmask;
- Gateway;
- Primary DNS and
- Secondary DNS.

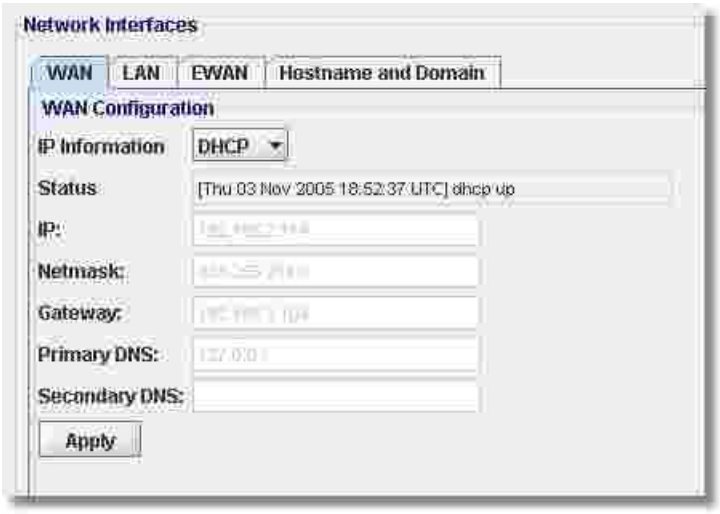
After entering this information, select “Apply”. Check the status returned.

© 2006 Critical Links, SA



DHCP

No additional information needs to be entered in this case, since all information is fetched from the DHCP server. Select “Apply” and check the status returned.



PPPoE

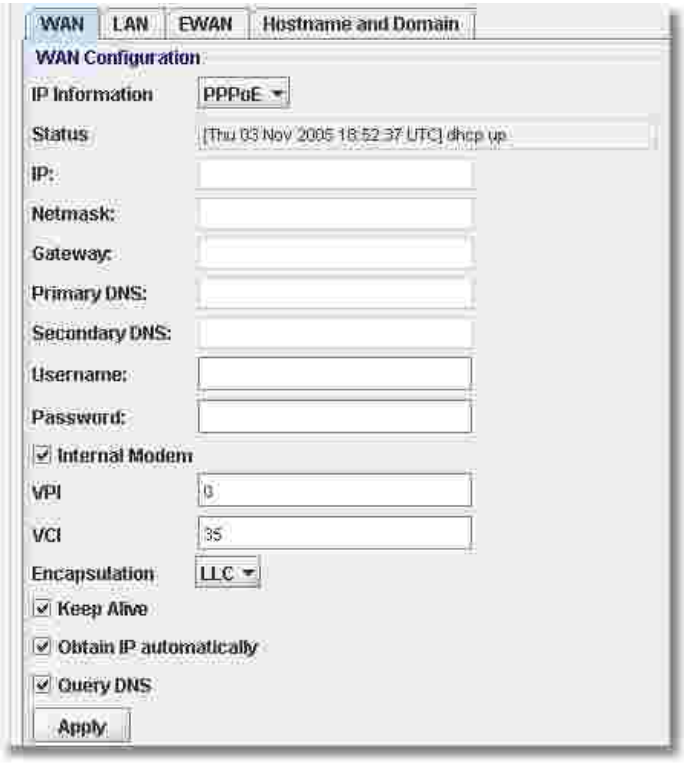
In this case, you are configuring an ADSL connection. You will have to provide the following information:

- IP address (this field will not be enabled if “Obtain IP automatically” is checked);
- Primary DNS and Secondary DNS (these fields will not be enabled if “Query DNS” is checked);
- Username/Password: This information will always have to be entered. Check the information your ISP has given you;
- Internal Modem: If this option is available, it means an internal modem is installed in your box. The following fields will also be enabled, and you will need to provide information on: VPI, VCI and Encapsulation. Check the information your ISP has given you;
- Keep Alive: Check this option if you want edgeBOX to keep trying to connect while a

© 2006 Critical Links, SA

connection is not successfully established; otherwise, edgeBOX will try for only 30 seconds;

- Obtain IP automatically: Check this option if you want the IP address to be fetched dynamically during connection setup;
- Query DNS: Check this option if you want DNS servers to be fetched on connection setup.



PPPoA

In this case, you are configuring an ADSL connection for an internal modem. Check PPPoE with an internal modem as the options listed there are similar.

UMTS

In this case you are configuring the gateway providing a connection to a UMTS or 3G cellular network. In addition to the fields specifying the IP address, Netmask, Gateway address and DNS servers that show the configuration of the WAN network interface, the following fields are used to configure the cellular connection:

- Pin: the identification number used to connect to the network;
- Protocol: currently IP is the only protocol supported;
- APN: the Access Point Name – a name used to identify the network to connect to, e.g. internet.company.com.
- OPSYS: is used to select the mechanism used to connect to the network:
    a. Only Connect to GSM Networks
    b. Only Connect to UMTS Networks
    c. If we have a choice GPRS first
    d. If we have a choice UMTS first
    e. Automatically let V3G decide.

© 2006 Critical Links, SA

This last option allows the network interface determine which network to connect to.

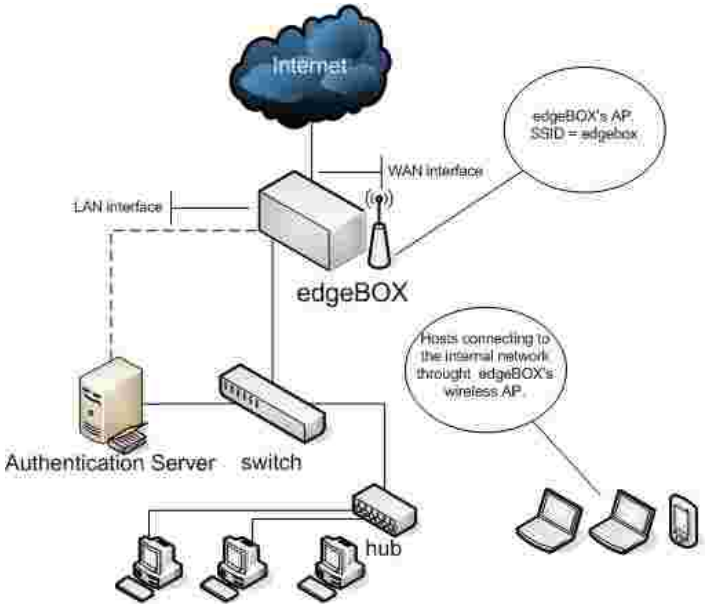
A box is also displayed showing details of the connection to the cellular network. Information on the registration number, network provider, network type, signal strength and connection status is displayed.

Note: Please contact technical support (edgebox.support@critical-links.com) to get the list of currently supported UMTS hardware.

None
In this case no information needs to be entered. The interface will be terminated.

Remember that if you change the configuration for the interface you are using to connect to the web based management console, you may need to reconfigure your client PC.

3.1.2 Wireless



edgeBOX's wireless AP

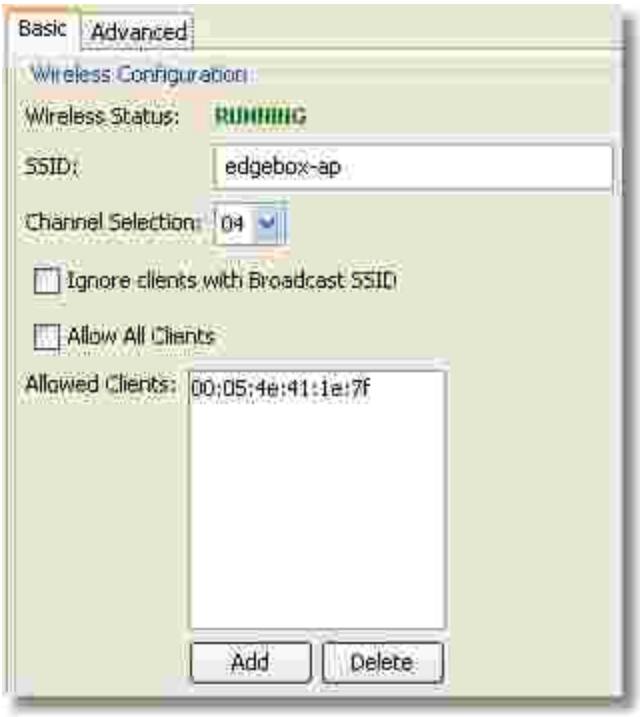
Through this menu option, you can review and change your wireless configuration. The actions available are togge the service state (Start/Stop) and Apply changes. These actions are available through the buttons in the lower panel. Possible scenarios for wireless configurations are depicted above. edgeBOX supports 802.1x authentication, allowing you to use its integrated authentication or use an external authentication server. Support for WPA is also included.

Wireless configuration is divided into two panels, accessed through their tabs: Basic and Advanced. Each of these panels is described next.

3.1.2.1 Basic

In this panel, you can configure general elements such as SSID, channel selection, whether to ignore clients with broadcast SSIDs or not and client access. Each of these options is described next.

© 2006 Critical Links, SA



3.1.2.1.1 Wireless Status

This element is read-only and shows you the service current state of the service. Possible values are Stopped and Running.

3.1.2.1.2 SSID

Public name for your wireless network.

3.1.2.1.3 Channel Selection

Select from the list. Available values are 1 to 12. If you experience signal degradation due to the interference with other devices nearby (other APs for example), you may need to change this setting.

3.1.2.1.4 Ignore clients with broadcast SSID

If selected, the SSID used by the client must exactly match edgeBOX's SSID (stations using no SSID i.e. stations that are "broadcasting" in search for an access point to associate to are not allowed to connect).

3.1.2.1.5 Allow all clients

If this option is checked, any client will be able to connect to the access point. If you uncheck this option, an “Allowed Clients” list will be visible. Each entry in this list will represent the MAC address of a PC that is allowed to connect to the access point. To manage this list you have two possible actions: Add and Delete.

Add

Adds a client to the list. After selecting this option a popup window will appear requesting you to enter the MAC address for the machine you want to allow to connection to the AP. After selecting “OK” you

© 2006 Critical Links, SA

have to select “Apply” in the main panel for changes to become effective.

Delete
Deletes a client from the list of allowed MACs, denying access to the PC with this MAC address. You will need to select “Apply” in the main panel for changes to become effective.

3.1.2.2 Advanced

In this panel, you can configure wireless security settings such as authentication and encryption.

3.1.2.2.1 Security Type

Select the security scheme to be used. Possible values are Static WEP keys, IEEE 802.1x and WPA.

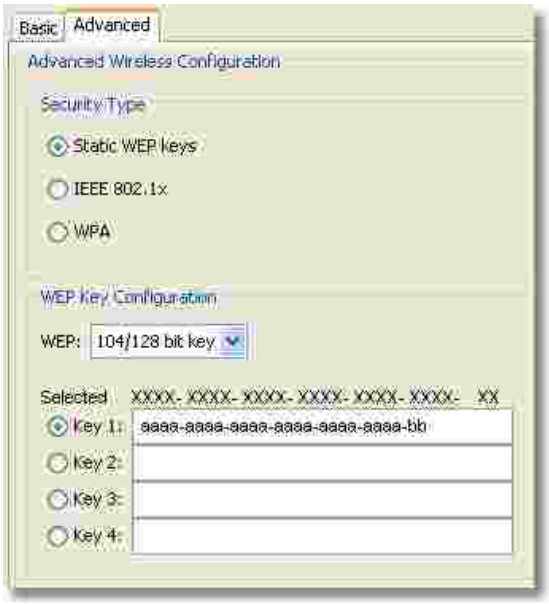
3.1.2.2.2 Static WEP keys

Choose from the list. Possible values are: None, 40/64-bit key and 104/128-bit key.

© 2006 Critical Links, SA

If you choose “none”, then encryption will not be enabled and your network will be vulnerable to connections from non-authorised hosts. With the other two options you are activating encryption and choosing the key length to be 64 or 128 bits. You may specify 4 different keys but only one may be active for transmission at a time. This key has to be distributed to clients who wish to connect to the network.

Bear in mind that this scheme is now relatively easy to break. To allow some degree of security keys should be changed regularly, which may not be manageable if there are many clients connecting to the access point.



Should WEP be used we advise you to at least configure one form of encryption.

3.1.2.2.3 IEEE 802.1x

In this panel, you may configure IEEE 802.1x authentication and encryption.

© 2006 Critical Links, SA

3.1.2.2.3.1 802.1x configuration

Use Remote Radius Server

Check this option if you want to use an external Radius server as the authentication server for IEEE 802.1x. You will need to provide the following:

- Radius Authentication IP: the external server's IP address;
- Radius Authentication Password: the external server's password;
- Radius Authentication Port: the external server's port.

If you leave this option unchecked, edgeBOX's Radius server will be used. With the new integrated authentication mechanism, the user's password to be used here will be the user's account password. Note that you will need to authorise access to wireless networking, during the user's account creation.

Radius Accounting

If you decide to use an external Radius server for authentication, you will also have the option of using an external Radius accounting server (which may not be the same one). You will have to provide the following:

- Radius Accounting IP: the external server's IP address;
- Radius Accounting Password: the external server's password;
- Radius Accounting Port: the external server's port.

© 2006 Critical Links, SA

3.1.2.2.3.2 Encryption type

Allows you to choose the encryption scheme to be used. Possible values are WEP and WPA.

WEP
If selected, dynamic session WEP keys will be used. During the authentication handshake, session keys are exchanged. These session keys are later used to compute dynamic keys, making encryption more difficult to crack.

WPA
If selected, WPA encryption will be used. Typically you will need to provide an initial key which will then be used to compute a temporal key, thus resulting in an unique key for each client-AP association. Care should be taken in choosing this key as a weak choice will make this scheme prone to dictionary attacks.Two options are available: Passphrase and PSK (Pre-Shared Key).

Passphrase
You will need to provide an ASCII passphrase.

PSK
You will need to provide a hexadecimal pre-shared key.

3.1.2.2.4 WPA

The options available here are covered in IEEE 802.1x's "Encryption type".

© 2006 Critical Links, SA

3.1.3 Routes

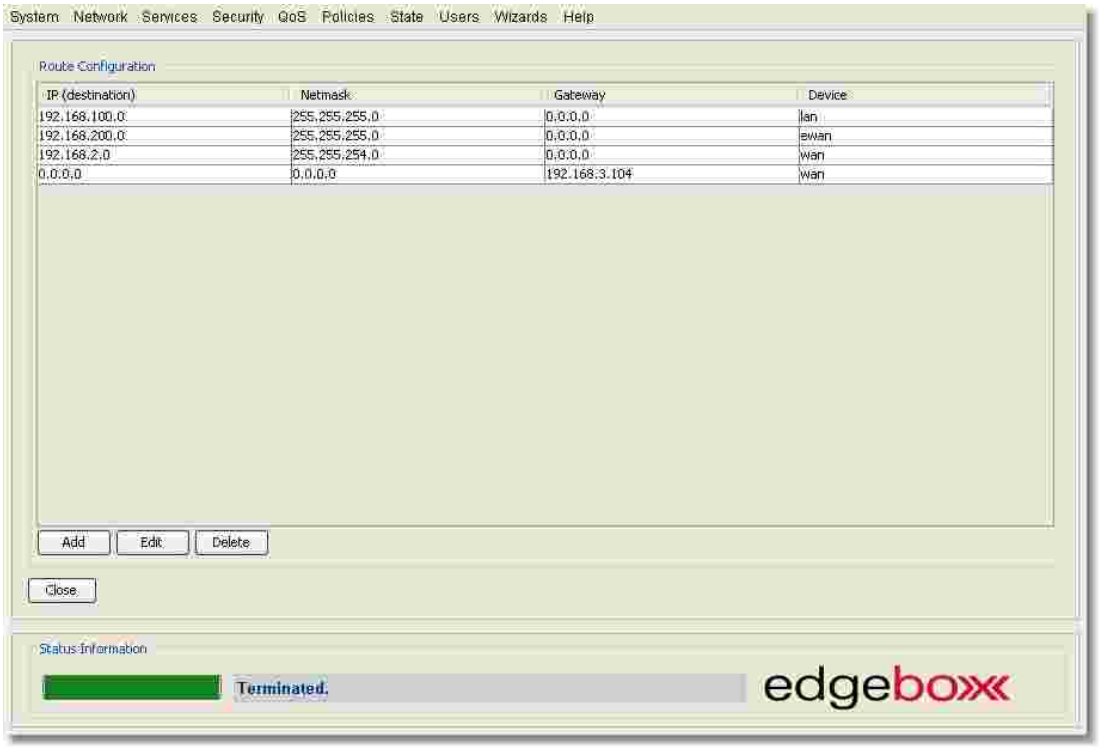
In this option, you can review and change your routes' configuration. Provided the interfaces were correctly configured you should not need to make any changes. After you run the setup wizard you may have the following entries in the route table:

- A route for your internal network; For example, if your internal network is 192.168.100.0/24, then you should have the following entry:
    - IP (destination): 192.168.100.0;
    - Netmask: 255.255.255.0;
    - Gateway: 0.0.0.0;
    - Device: LAN (this is the internal network interface).
- A route for your enterprise network; If your enterprise network is 192.168.100.200.0/24, then you should have the following entry:
    - IP (destination): 192.168.200.0;
    - Netmask: 255.255.255.0;
    - Gateway: 0.0.0.0;
    - Device: EWAN (this is the enterprise interface);
- A route for your WAN network, where the gateway to access the Internet is located. For example, if the network is 192.168.170.254/32 (e.g. a point-to-point link), the entry may be:
    - IP (destination): 192.168.170.254;
    - Netmask: 255.255.255.255;
    - Gateway: 0.0.0.0;
    - Device: WAN.
- A default route; this is typically the gateway address present in the WAN configuration, the one used to access the Internet. For example, if your gateway has the IP address 192.168.170.254, then the entry will be:
    - IP (destination): 0.0.0.0;

© 2006 Critical Links, SA

- Netmask: 0.0.0.0;
- Gateway: 192.168.170.254;
- Device: WAN.

Should you need to manually edit edgeBOX's routing table, the operations available are Add, Edit and Delete.



3.1.3.1 Add

To add a new route, follow these steps:

- Select “Add”;
- Enter the following information:
  - - IP (destination): the destination network/host;
  - - Netmask: the netmask to apply;
  - - Gateway: the gateway to use to reach the network/host and
  - - Device: the interface to use. Choose from the list.
- Select “OK”. Check the status returned.

3.1.3.2 Edit

To modify an existing route, follow these steps:

- In the route table, select the desired route and press the Edit button (you may also double click);

© 2006 Critical Links, SA

- Change the desired information;
- Select “OK”. Check the status returned.

3.1.3.3 Delete

To delete an existing route, follow these steps:

- In the routing table, select the route to delete;
- Select “Delete”.
- Check the Status returned to see if the operation was successful.

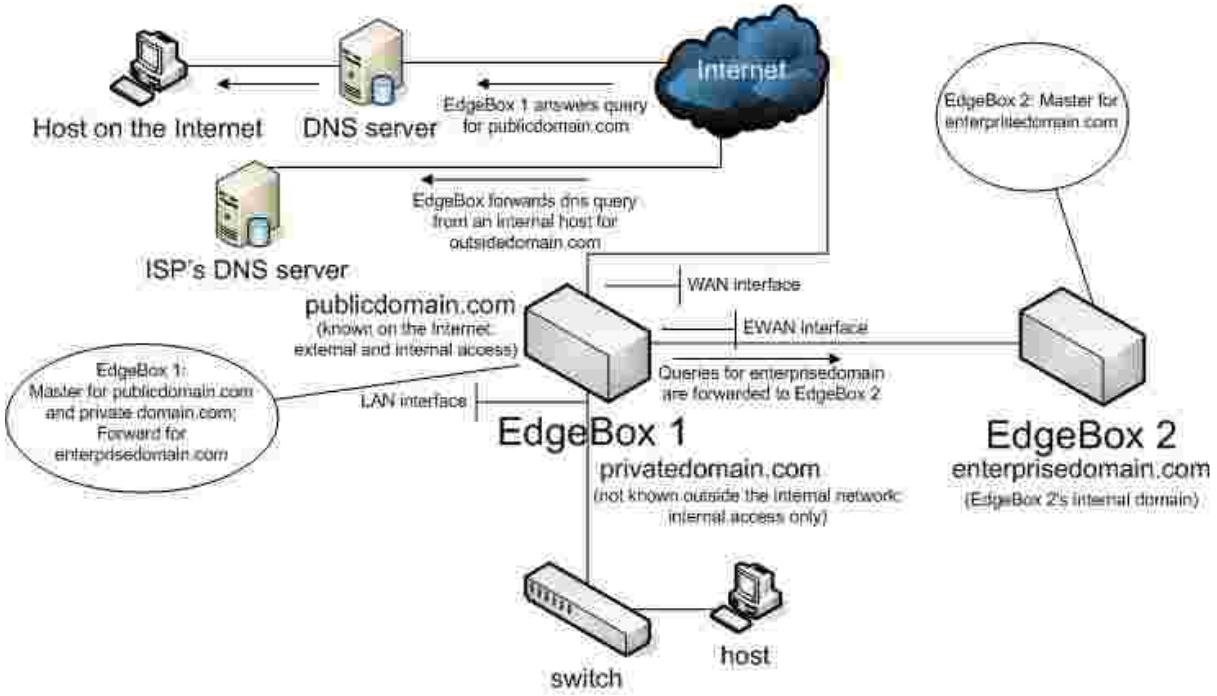
3.2 Services Menu

This menu option allows you to review and configure the settings for the services running on edgeBOX, namely:

- DNS;
- Dynamic DNS;
- DHCP;
- HTTP;
- SMTP;
- Samba;
- Web filtering and
- VoIP.

© 2006 Critical Links, SA

3.2.1 DNS



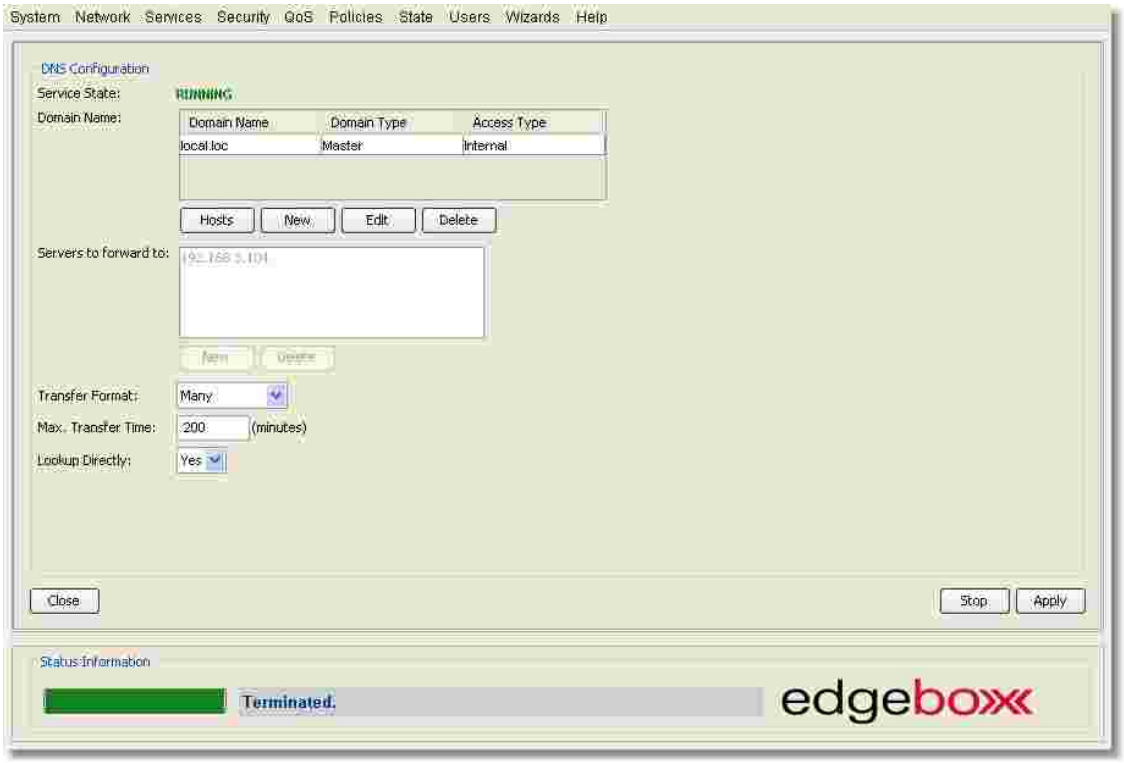
DNS configurations supported by edgeBOX

In this option, you can review and change your DNS configuration.

DNS (Domain Name Server) is a service that looks up information related to a domain. edgeBOX supports DNS through the well-known *named* server. It is possible to configure master and forward type name servers, as well as granting query access from internal or external networks. In the main panel, you have the options, which you may configure. On the bottom, you have two buttons, corresponding to two different actions:

- Stop/Start: The caption on this button will change depending on the service status; this button allows you to toggle its status.
- Apply: This button allows you to change the configuration, while keeping the current service status.

© 2006 Critical Links, SA



DNS configuration page

Next, we will describe each element present in the main panel.

3.2.1.1 Service State

This item is read-only and provides information on the status of the service, i.e. if it is started or stopped.

3.2.1.2 Domain Name

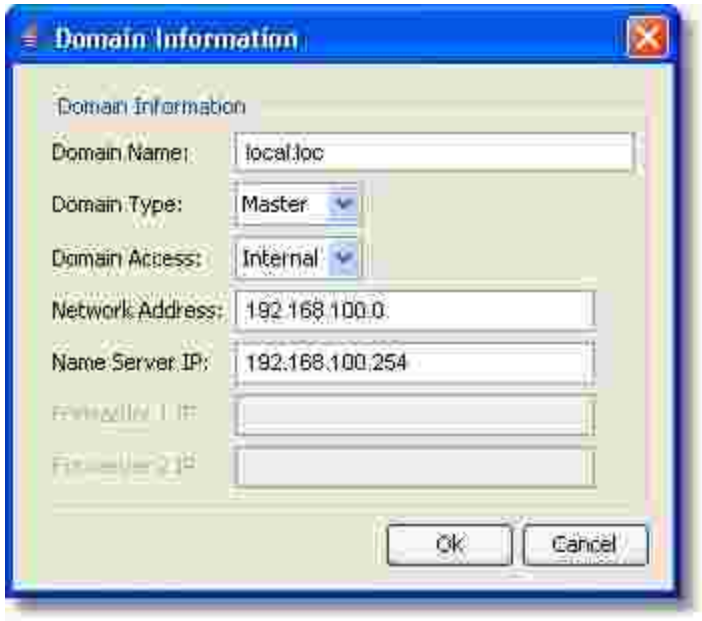
In this table you have the list of domains configured, their type and access type. After you run the wizard, at least one entry should be shown here – the one corresponding to the local private domain. edgeBOX automatically creates the forward and reverse zones, and a set of hosts, depending on the configuration entered.

The available options are Hosts, New, Edit and Delete.

© 2006 Critical Links, SA

3.2.1.2.1 New

This option allows configuration of a new domain. After you select this option a pop-up window will appear requiring you to enter the following information:



New Domain Window

- Domain Name: the name of the new domain;
- Domain Type: Select a value from the list. The available selections are Master and Forward. A master domain server is one which has the database for the domain stored locally (also called authoritative domain for that domain). It will answer the queries for that domain. A forward domain server does not answer queries directly, but will forward them to another name server.
- Domain Access: Select a value from the list. The available selections are Internal and External. If you have a registered domain you will grant access to external networks to query this zone; otherwise for private domains you will most likely want to grant only to internal hosts for security reasons. This option is disabled for forward-type name servers.
- Network mask: The network mask used for this network. This value will be used to build the reserve zone;
- Name Server IP: The IP for this domain's name server. This option is disabled for forward-type name servers;
- Forwarder 1 IP/Forwarder 2 IP: If you've chosen type “Forward” this will be the IP addresses of the servers where queries for this domain will be forwarded.

3.2.1.2.2 Edit

Allows you to change the configuration for an existing domain. Select the domain to edit and select “Edit”. The options available are similar to the ones available when creating a new domain.

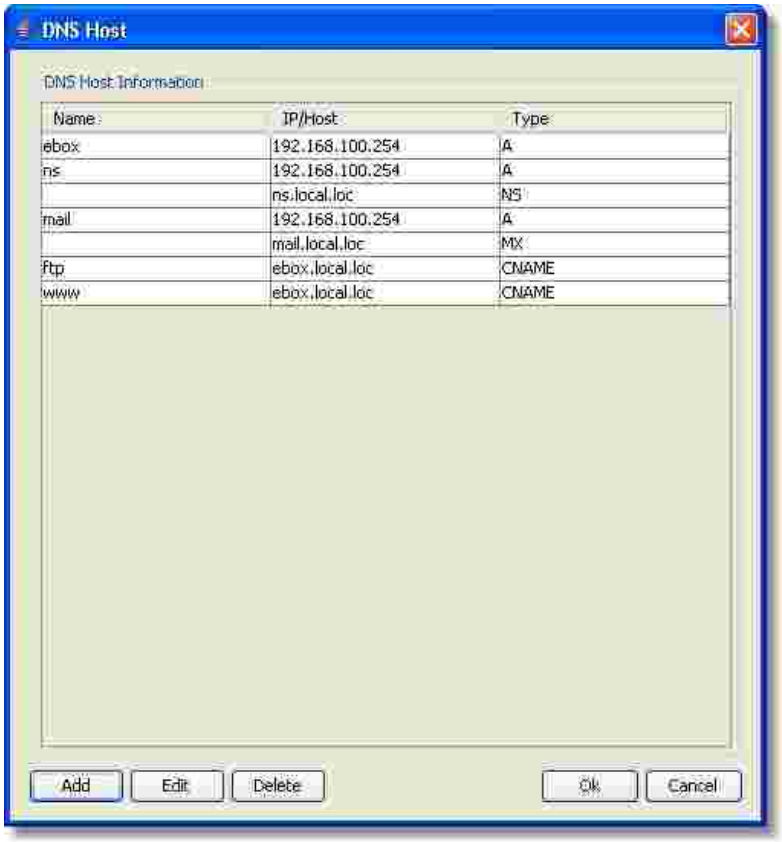
3.2.1.2.3 Delete

Deletes configuration information for a selected domain. Select the domain to delete and select

© 2006 Critical Links, SA

"Delete". Check the status returned by this option.

3.2.1.2.4 Hosts



This option allows management of the domain database. After selecting the domain and pressing "Hosts", a new pop-up window will appear. In this window there is a table with all the entries for this domain database. Available actions are:

Add Host Window

Add

© 2006 Critical Links, SA

Allows you to add a new entry. A dialogue panel will be displayed requiring you to enter the following information:

- Host Name: the name of the host to be added;
- Host Type: Select from the list. Available choices are A, CNAME, MX and NS.
- Host IP: the IP for this host.

Edit
Allows you to change a record's information. The options available are the same as in "Add".

Delete
Deletes an entry from the database. Select the entry to delete and press “Delete”.

Remember that any of the changes made to the domain(s) database will only take effect after you select “Apply” in the main panel; if you don't select “Apply” then all changes will be lost.

3.2.1.3 Servers to forward to

This list contains the servers to where queries will be forwarded to if the domains queried are not in the list of domains. This will be the Name Server(s) used to resolve external domains. You will only be able to change this setting if you have a static configuration on the WAN side – otherwise this list is populated automatically from the information fetched from the DHCP or PPP server on connection setup. There are two actions possible:

New
A pop-window will appear. Just enter the IP address for the Name Server.

Delete
Select the Name Server IP and then select “Apply” for the changes to become effective.

3.2.1.4 Transfer Format

Select a value from the list. Available values are: “One at a time” and “Many”.

Determines the format used by the server to transfer zones: many will pack as many records as possible into a maximum sized message, whereas one will place a single record in each message.

3.2.1.5 Max Transfer Time

Maximum time allowed for inbound zone transfers.

3.2.1.6 Lookup Directly

Select a value from the list. Allowed values are: Yes/No.

If set to “Yes” and a query sent to a forwarder isn't answered, the server will try to answer it. If set to “No” the server will forward queries to forwarders only.

© 2006 Critical Links, SA

3.2.2 Dynamic DNS

This panel allows you to configure the edgeBOX built-in client for Dynamic DNS services.

This kind of service is usually used when you don't have a static IP configuration on the WAN side and still want to access your machine by a name of your choice. The edgeBOX supports DynDNS (http://www.dyndns.org) and No-IP (http://www.no-ip.org) dynamic DNS services. Details on how to setup and manage an account on these services are out of the scope of this text and the user is directed to the URLs given. The available configuration information includes:

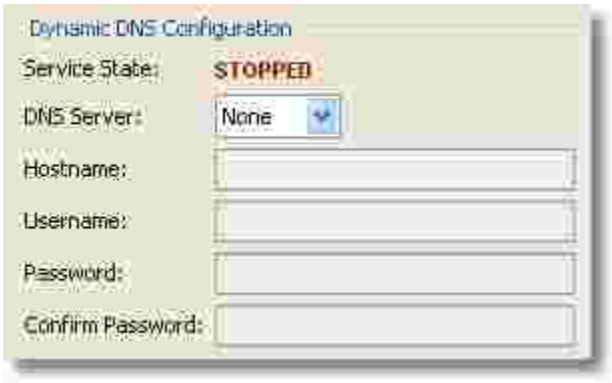
DNS Server
The type of service used. Select from the available choices' list: None, DynDNS or No-IP.

Hostname
The name you want to use. This hostname must have been previously created. For details on managing hostnames, please check the documentation for the dynamic DNS service chosen. The full-qualified domain name will be hostname.no-ip.org or hostname.dyndns.org.

Username
The username for the account used for accessing the service chosen;

Password
The password for the account used for accessing the service chosen;

For the changes to become effective, you have to select “Apply”. Please check the status returned to see if the operation was successful.



3.2.3 DHCP

This service is available for the internal network only, and is used to dynamically assign IP address to hosts on the internal network. Only two actions are possible: Starting and Stopping the service. We will now describe the elements available on the main panel.

© 2006 Critical Links, SA

3.2.3.1 Service State

This information is read-only and provides the service status (i.e. running or stopped).

3.2.3.2 Domain name

This information is also read-only – it provides the internal domain name.

3.2.3.3 Ranges

This panel defines the range of IP addresses that will be assigned dynamically. You may define several address intervals as long as they don't overlap. For each address interval defined, you can define a prefix that will be added to the last portion of the IP assigned to form the hostname sent. The operations available are New and Delete.

© 2006 Critical Links, SA

3.2.3.3.1 New

New DHCP Range window

After selecting “New”, a pop-up window will appear. The following information must be entered:

- Start IP: Lower end of the IP address interval;
- End IP: Higher end of the IP address interval;
- Prefix: String to be concatenated to the address sent, to form the hostname. For example, if you enter “mobile“ for the prefix, and the domain is called “local.loc”, then the host with IP address 192.168.100.200 will have the hostname “mobile-200.local.loc”.

3.2.3.3.2 Delete

After selecting the interval to remove, press “Delete”. Check the status returned to confirm the operation completed successfully.

3.2.3.4 MAC-IP

This panel defines relations between MAC addresses and IP addresses. Host machines whose MAC address is listed here may still fetch the IP dynamically; however, this value will always be the same. The actions available are New and Delete

3.2.3.4.1 New

After selecting “New”, a dialogue panel will be displayed. The following information must be provided:

- MAC address: the network card address. To find this address, you may use the command ipconfig /all (in windows) or ifconfig (in UNIX).
- IP address: the IP address to be assigned.

  After selecting “OK”, check the status returned to confirm the operation was successful.

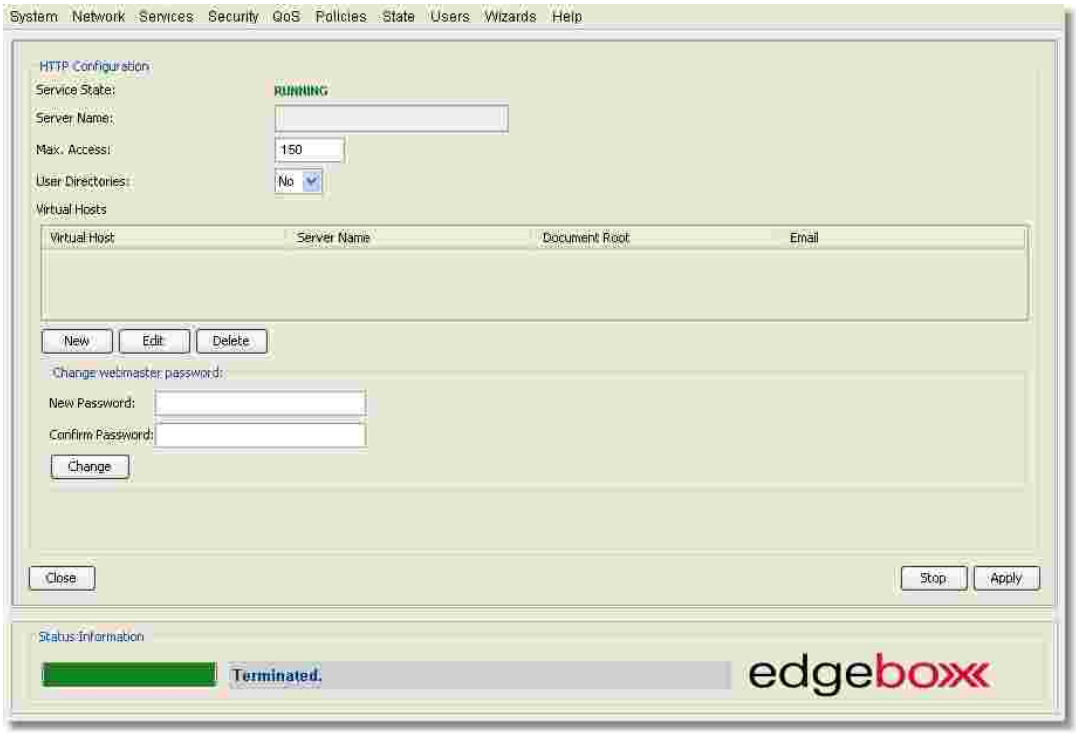
© 2006 Critical Links, SA

3.2.3.4.2 Delete

Select the MAC-IP relation you want to eliminate and then select “Delete”. Check the status to confirm the operation was successful.

3.2.4 HTTP

In this panel you can review and change the configuration for the http service running on edgeBOX which is provided by an Apache web server. Two actions are possible, performed with the two buttons on the bottom-most panel: toggle service status (Start/Stop) and apply changes made to the configuration (button “Apply”). The available configuration options are described next.



3.2.4.1 Service State

This element is read-only and has the current status for the http server: Running or Stopped.

© 2006 Critical Links, SA

3.2.4.2 Server Name

This information is read-only.

3.2.4.3 Max. Access

Here we set the maximum number of simultaneous access connections to the web server.

3.2.4.4 User Directories

Select from the list. Possible values: Yes/No. If set to “Yes” users will have a personal web page. That homepage will be located on the user's home directory under the public_html directory. The user will be able to manage their personal webpage through FTP – after logging on they will be placed in this directory automatically. The URL to access a user's personal webpage will be formed from the concatenation of the main URL with “~username”. For example, if the main URL is http://edgebox.domain, then noname's webpage will be located on http://edgebox.domain/~noname or http://edgebox.domain/users/noname.

3.2.4.5 Virtual Hosts

This panel allows you to configure virtual hosts. With virtual hosts, you are able to have the same web server running multiple websites. Possible actions are New, Edit and Delete.

3.2.4.5.1 New

After selecting the “New” button, a popup window will appear, requesting that you enter the following information:

- Virtual Host. Select from the list of values. Possible values are: LAN, WAN and both. Defines the scope of access to this virtual host.
- Server Name: The name of this virtual host. Remember that an A or CNAME record has to be added to the DNS for this setup to be complete. For example, if your domain is local.loc, and you add a virtual host for “docs.local.loc”, then you will have to add an entry for host “docs” pointing to edgeBOX’s IP address.
- Document Root: the location of the files in the file system. All websites will be located under /home/wwwhost, which is the filesystem directory where the webmaster user will be placed after logging on through FTP. The Document Root is specified relative to this directory. For example, the document root for the intranet website is “intra”. Taking the example from the previous option, if you create a directory under “/home/wwwhost” called “documents” to place the virtual host files’, then the document root will be “documents”.
- Email: the email for the responsible for this domain.

© 2006 Critical Links, SA

3.2.4.5.2 Edit

This option allows you to change a Virtual host configuration. The fields available are the same as for the new virtual host window.

3.2.4.5.3 Delete

An entry has to be selected. To make this change effective, select “Apply”.

3.2.4.6 Change Webmaster password

This option allows you to change the password for user 'webmaster'. The user 'webmaster' has FTP access and owns the directory tree for the intranet and Internet websites. The FTP root directory will initially contain two directories (“intra” and “inter”), corresponding to these websites, but more may be created, for example for virtual hosts’ websites.

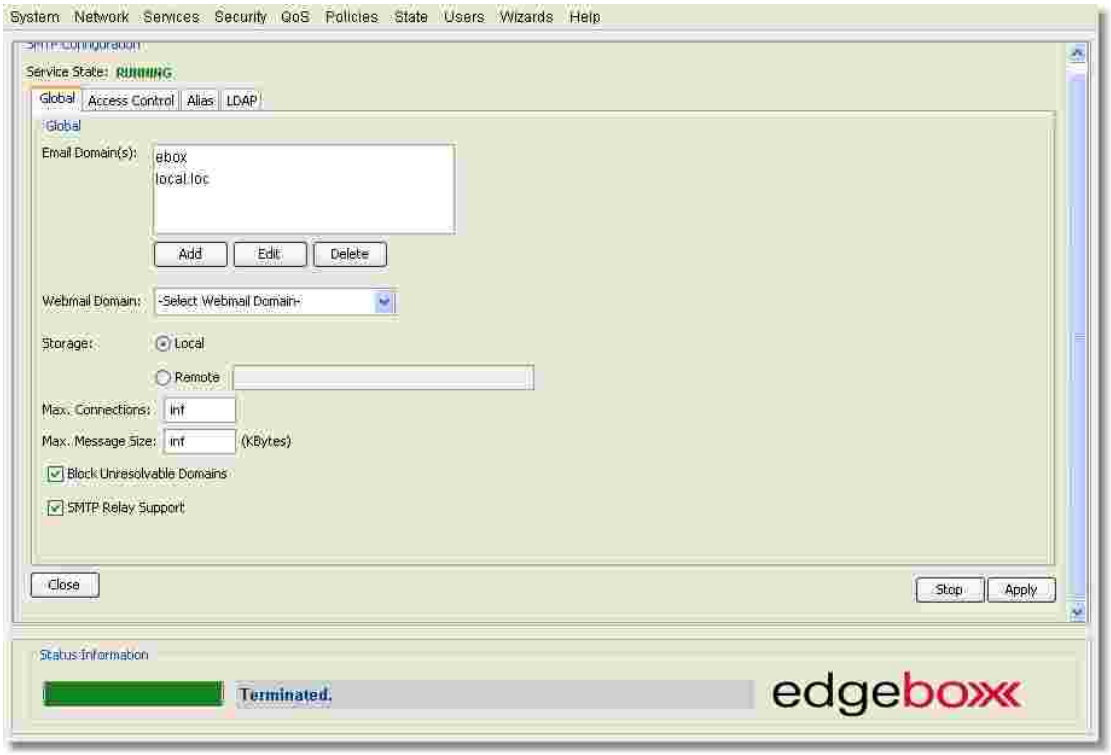
To change the password, type the password in the “New Password” and “Confirm Password” fields, and select the button “Change”. Remember that this account is initially disabled so you will have to set a password in order to use it.

3.2.5 SMTP

This page allows you to review and change your mail server configuration. The edgeBOX implements this service using Sendmail. Again, the actions available are toggling the service state (Start/Stop) and applying (Apply) changes.

There are two buttons on the lower panel that trigger these actions when selected. The following panels are available: Global, Access Control, Alias and LDAP. Each of these panels is selected using the appropriate tab and is described in the following sections.

© 2006 Critical Links, SA



3.2.5.1 Service State

This element is read-only and shows the current service status (running or stopped).

3.2.5.2 Global

In this panel, you can configure general email options, such as:

- Email domain(s) for which you will be receiving email;
- Type of storage used;
- Max. simultaneous connections;
- Max. message size;
- Blocking of unresolvable domains and
- Support for SMTP relay.

© 2006 Critical Links, SA

3.2.5.2.1 Email Domain(s)

A list with the alternate hostnames for this host and domains for which it will accept mail. Each entry has to be a full-qualified domain name. Available actions are “Add”, “Edit” and “Delete”.

Add
After selecting this option, enter the Domain name select OK then click on the Apply button to make this change effective.

Edit
Allows you to modify the selected entry. To make this change effective, don't forget to select the "Apply" button.

Delete
Select the entry you want to delete and then click on “Delete”. Don't forget to click “Apply” to make this change effective.

3.2.5.2.2 Webmail Domain

Allows you to choose the domain which you want to set as your webmail domain. Only one domain may be a web mail domain. For details on using and accessing the web mail functionality, check Web Mail.

3.2.5.2.3 Storage

If you choose 'local', then all mail will be stored on edgeBOX; if you choose 'remote', you will have to provide a hostname to which all mail will be relayed.

© 2006 Critical Links, SA

3.2.5.2.4 Max. Connections

The maximum number of simultaneous connections. After this number, connections will be rejected. If set to 'inf' then there will be no limit.

3.2.5.2.5 Max. Message Size

The maximum size of messages that will be accepted. Setting it to 'inf' will accept messages of any size.

3.2.5.2.6 Block Unresolvable Domains

Checking this option will cause all mail that arrives from un-resolvable domains to be refused. This is the default behavior for security reasons (as this is a very common technique used by spammers).

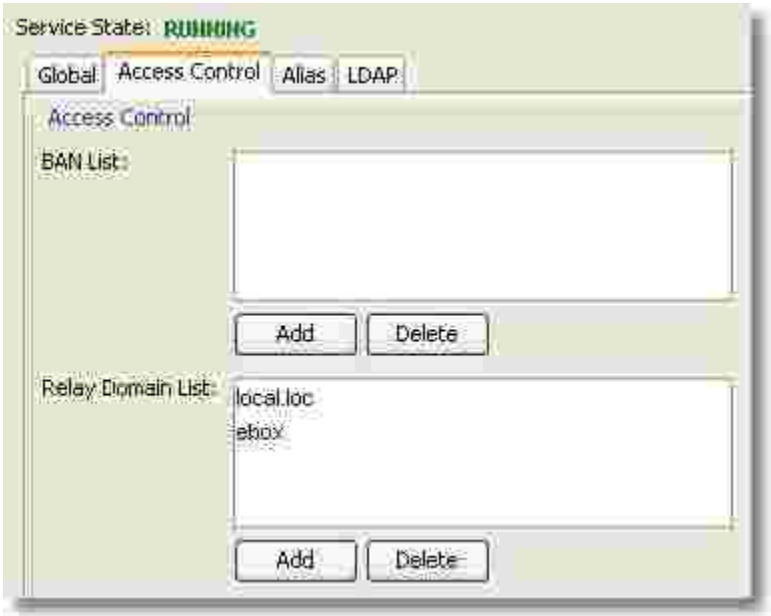
3.2.5.2.7 SMTP Relay Support

Checking this option means that you are allowing relay from users authenticated through POP3. This will be a limited authorisation, as it will expire some time later. This setting is particularly useful for users who are connecting from external networks (while, traveling for example, the so called “Road Warriors”) and for which we want to allow relaying. Bear in mind that you will have to grant access to the POP3 service from outside networks in the firewall configuration.

3.2.5.3 Access Control

In this panel, you will be able to configure access control options, such as:

- The list of banned domains/hosts and
- The list of relay domains.



© 2006 Critical Links, SA

3.2.5.3.1 Ban List

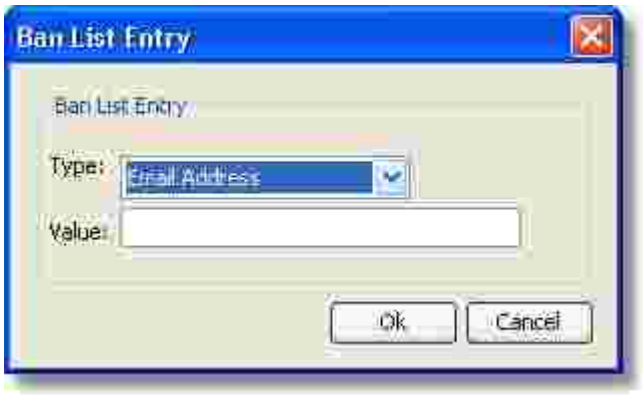
A list with email addresses, host IPs, domains or hosts for which connections will not be accepted. Available actions are “Add” and “Delete”.

Add

After selecting “Add”, a popup window will appear and you are required to select the type of entry you wish to add from the list of available types: "Email Address", "Host", "Network IP Address", "Hostname" and "Domain". When entering a value, you may use wildcards (“*”). If a given domain is listed all sub domains will be banned. After selecting “OK” you have to select “Apply” in the main panel to make the changes effective.

Delete

Select an entry from the list and select “Delete”. To make this change permanent select “Apply” from the main panel. Eliminating an entry from this list means that you are allowing connections from that entry.



3.2.5.3.2 Relay Domain List

A list with domains or hosts that will be allowed to relay mail. Relaying is denied for hosts on the Internet; with this list, you can configure a list of trusted domains or hosts which you are willing to relay mail for. Two actions are possible: “Add” and “Delete”.

Add

After you select “Add”, a popup window will appear, requesting the domain or host name. After selecting “OK”, you have to select “Apply” on the main panel for changes to become effective.

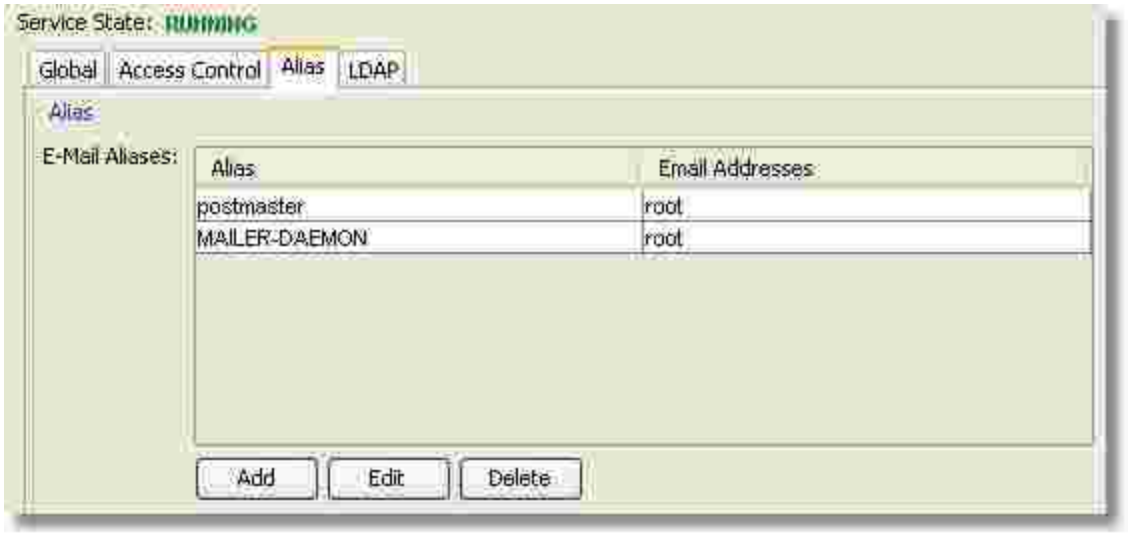
Delete

Deletes an entry from the relay domain's list. After selecting the domain you want to eliminate (and thus deny relaying again), select “Delete”. You then have to select “Apply” in the main panel for this change to become effective.

3.2.5.4 Alias

In this panel, you may edit the aliases' list.

© 2006 Critical Links, SA



3.2.5.4.1 E-Mail Aliases

With this element you can provide alternate names for individual users, forward mail to another host or create mailing lists. This table has some predefined aliases related with management. You can choose to redirect mail for these aliases to another user, so that they receive the notifications. You may also define more descriptive names for your users instead of your 8-letter login names. Each entry has on the first column the alias name, and on the second column the email address to which it will expand. There are two operations available: “Add” and “Delete”.

Note: the root alias will not appear on this list as it is configured elsewhere (System menu, Config submenu).

Add

If you select this operation, a popup window will appear requesting the following information:

- Alias: the name of the alias you want to create;
- Email(s): the email or list of emails to which this alias will expand.
- After selecting OK, don't forget to select “Apply” so the changes become effective.

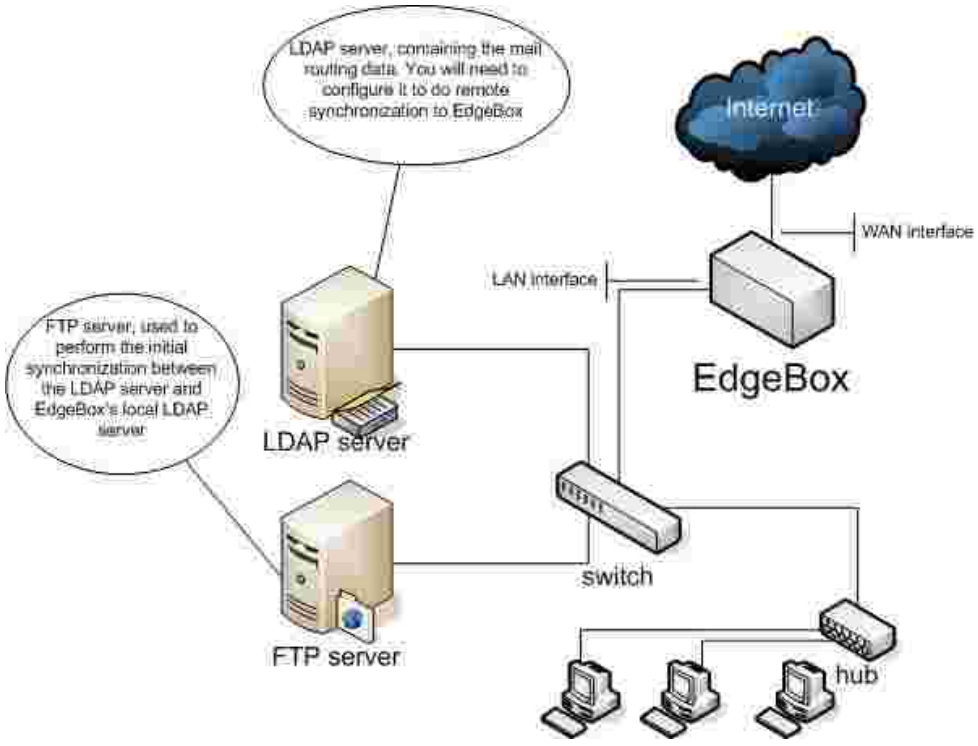
Delete

To delete an alias, select it from the list and press “Delete”. Don't forget to select “Apply” to make this change effective.

© 2006 Critical Links, SA

3.2.5.5 LDAP

In this panel you can configure the mail server to perform LDAP-based rerouting of a particular address to either a different host or a different address. edgeBOX's LDAP mail routing function follows the "LDAP Schema for Intranet Mail Routing" Internet-Draft Document. Initially you will have to perform synchronization between the LDAP server, which holds the mail routing data and the local LDAP server running on edgeBOX. This synchronisation is done via FTP. The remote LDAP server must be configured to perform replication to edgeBOX's local LDAP server.

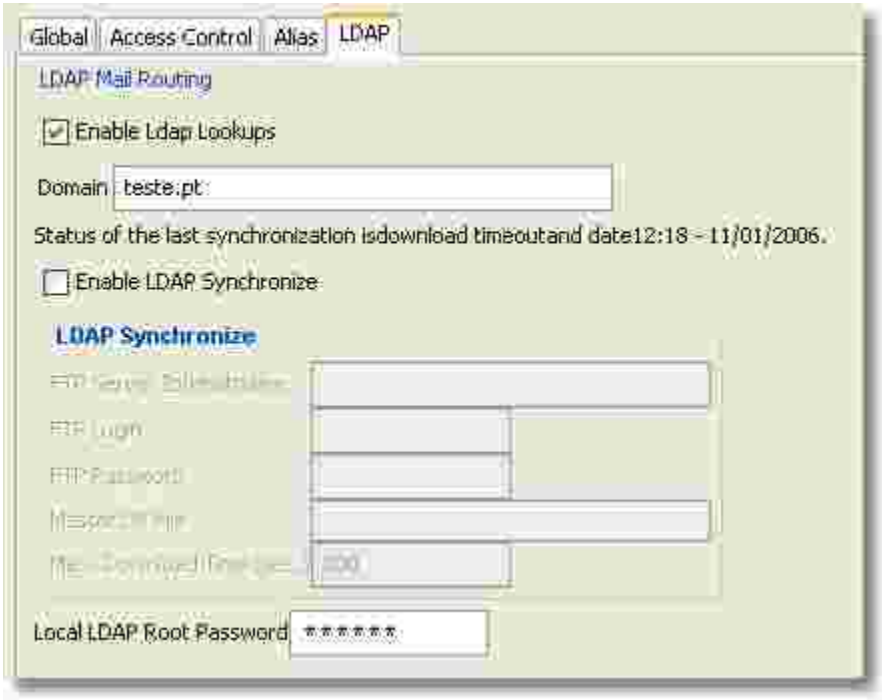

LDAP server, containing the mail routing data. You will need to configure it to do remote synchronization to EdgeBox
Internet
WAN interface
LAN interface
EdgeBox
FTP server, used to perform the initial synchronization between the LDAP server and EdgeBox's local LDAP server
LDAP server
switch
FTP server
hub

© 2006 Critical Links, SA

3.2.5.5.1 LDAP Mail Routing

The following options are available:

- Enabling LDAP lookups;
- The domain;
- Enabling LDAP synchronisation and
- Setting the local LDAP root password.



3.2.5.5.1.1 Enable LDAP Lookups

Checking this option will enable LDAP routing of email traffic. The remaining options will then be available for configuration.

3.2.5.5.1.2 Domain

The domain for which we will be doing LDAP routing; enter a full qualified domain name – this domain will then be broken in DCs (domain components) which will be used by LDAP.

3.2.5.5.1.3 Enable LDAP Synchronize

Checking this option will enable you to configure the options for performing the initial synchronisation. You will be required to enter the following information:

- FTP Server IP/Hostname: The IP address or hostname for the remote server where the LDAP DB file is located;

© 2006 Critical Links, SA

- FTP Login: Username used to log in to the remote FTP server;
- FTP Password: Password for the username used;
- Master DB File: The file holding LDAP data in LDIF format;
- Max. Download Time (sec.): The maximum amount of time for the transfer to be completed; if this time is exceeded, the transfer will be aborted.

3.2.5.5.1.4 Local LDAP Root Password

The password used by the remote LDAP server to perform synchronisation on the local LDAP server. The remote LDAP server has to be configured to perform replication to edgeBOX. The following remarks should be taken into consideration when configuring the remote LDAP server:

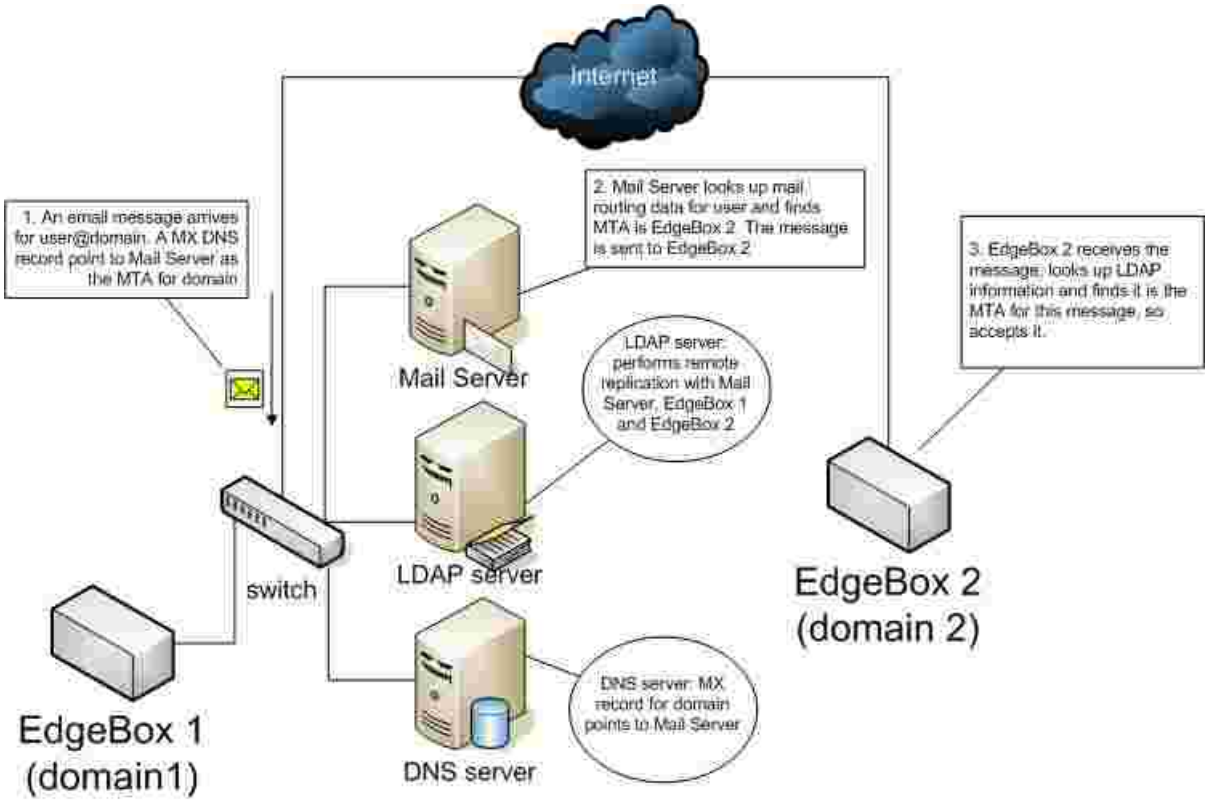
- Only the core and miscellaneous schemas shall be configured to be replicated;
- A replica section has to be included in the configuration file, where:
  - The URI points to the local edgeBOX;
  - The TLS element is set to “critical”;
- The cn (common name) used in the binddn (distinguished name) has to be set to “manager”;
- The credentials element has to be set to edgeBOX's local LDAP server root password;
  For example, if the domain is local.loc, the edgeBOX is located on 192.168.100.254, and edgeBOX's LDAP server root password is “secret”, then the replica section will look like:

```
replica uri=ldap://192.168.100.254
tls=critical
binddn="cn=Manager,dc=local,dc=loc"
bindmethod=simple credentials=secret
```

Important note: You will need a certificate in order to perform replication between the master LDAP server and edgeBOX’s local LDAP server, since we’re using TLS to perform this replication. You will need to download the certificate file located at http://192.168.100.254/certs.

Remember that you will have to select the “Apply” button for changes to become effective.

© 2006 Critical Links, SA


Internet
1. An email message arrives for user@domain. A MX DNS record point to Mail Server as the MTA for domain
2. Mail Server looks up mail routing data for user and finds MTA is EdgeBox 2. The message is sent to EdgeBox 2
3. EdgeBox 2 receives the message, looks up LDAP information and finds it is the MTA for this message, so accepts it.
Mail Server
LDAP server: performs remote replication with Mail Server, EdgeBox 1 and EdgeBox 2
LDAP server
switch
EdgeBox 2 (domain 2)
EdgeBox 1 (domain1)
DNS server: MX record for domain points to Mail Server
DNS server

A possible LDAP Mail Routing scenario

3.2.6 Samba

The Samba service allows edgeBOX to interact with other hosts as if it was a Windows server. Besides the usual file and printer sharing services, edgeBOX's may also act as a PDC and WINS server.

WINS performs name registration and resolution. Windows clients can query a WINS server directly, instead of using the usual broadcast method, thus resulting in an improvement in performance (the hosts don't need to process broadcast packets).

When edgeBOX acts as a PDC, users' desktop preferences are stored in edgeBOX (roaming profiles), and their home directory is mounted locally as Z: drive.

The service is provided to all authorised users listed on the Users panel.

The following panels are available, each accessible through its tab: Global, Shares, Homes, Boxes and USB Printers.

© 2006 Critical Links, SA

3.2.6.1 Service State

Reports the current state of the Samba service: Stopped or Running. If the service is Stopped it can be started by clicking on the Start button at the bottom right hand corner of the panel. Similarly if the service is Running it can be stopped by clicking on the Stop button.

3.2.6.2 Global

This panel allows you to configure general Samba settings such as Workgroup name, server string, WINS and PDC options.

3.2.6.2.1 Global

This section is used to make the Samba service accessible to Windows clients.

Workgroup
The name of the Windows workgroup that Windows clients must belong to access the services provided.

Server Name
A brief description of the edgeBOX server to make it easier to identify when browsing the network.

Wins Support
If you check this option, edgeBOX will act as a WINS server, providing WINS name service registration and resolution. An additional options panel will allow you to configure its role.

PDC Support
If you check this option, edgeBOX will act as a Windows Primary Domain Controller. After aplying,

© 2006 Critical Links, SA

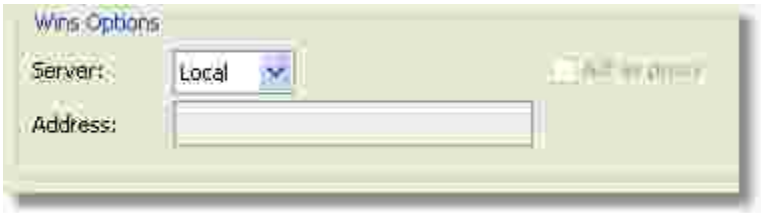
the SID for this domain will be visible next to the Workgroup.

3.2.6.2.2 Wins Options

Server
Available options are Local or Remote. If set to Local, edgeBOX will act as a WINS server.
If set to Remote, edgeBOX will use a remote WINS server. In the later case, the following options will also be enabled:

Act as Proxy
If you check this option, edgeBOX will act as a WINS proxy, relaying registration and resolution requests from itself to another WINS server. edgeBOX will send the response back to the original client.

Address
Allows you to specify the IP address for the remote WINS server to be used.



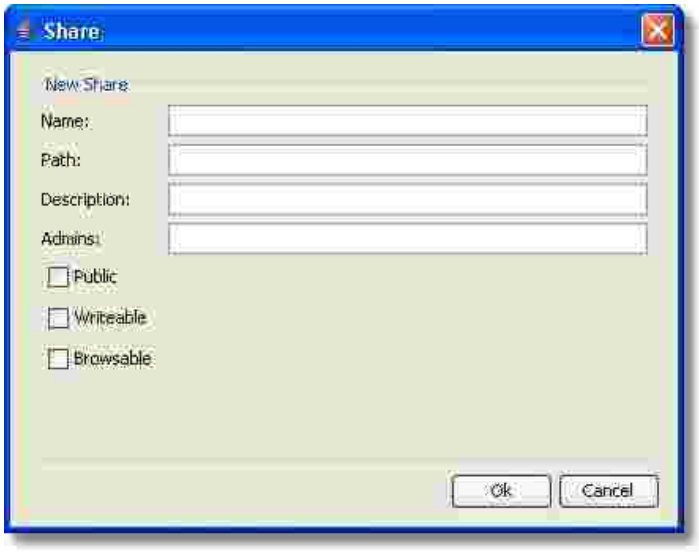
3.2.6.3 Shares

Displays a list of the shared folders that are currently active. New shared folders can be created by clicking on the New button, access permissions can be changed by selecting a shared folder and clicking on the Edit button; shared folders can be deleted by selecting an item from the list and clicking the Delete button.

3.2.6.3.1 New

When the New button is clicked the New Share panel is displayed. It contains the following fields.

© 2006 Critical Links, SA



Name
Enter the name of the shared directory. This name is used to allow users map the folder into their filesystem.

Path
The name of the folder on the edgeBox filesystem. A single folder name is specified. Folders cannot be nested.

Description
A brief description of the folder and what it contains.

Admins
A list of user names, separated by semi-colons, that are allowed to administer the shared folder, e.g. admin;bob;sarah.

Public
Check this box if the shared folder is publicly accessible.

Browseable
Check this box if the shared folder can be browsed.

Writeable
Check this box if the shared folder can be written to.

3.2.6.3.2 Edit

When the Edit button is clicked to change the properties of an existing shared folder the Edit Share panel is displayed. It contains the following fields.

Name
The name of the shared directory. This field is disabled and cannot be changed.

Path

© 2006 Critical Links, SA

The path to the folder on the edgeBOX file system. This field is disabled and cannot be changed.

Description
A brief description of the folder and what it contains.

Admins
A list of user names, separated by semi-colons, that are allowed to administer the shared folder, e.g. “admin;bob;sarah”.

Public
Check this box if the shared folder is publicly accessible.

Browseable
Check this box if the shared folder can be browsed.

Writeable
Check this box if the shared folder can be written to.

3.2.6.4 Homes

Authorised users can have a home directory on the edgeBOX. The home directory works as a network folder only accessible to the user.

Active
Activates the home directories for authorised edgeBOX users. The amount of space available to each user may be controlled by setting disk space quotas.

Browseable
Allows other edgeBOX users read-only access to users' home directories.

3.2.6.5 Boxes

Boxes are a great way to allow users to exchange files using a temporary folder. Boxes can be request via the edgeBOX Services web page.

Active
Activates the Boxes service.

Size Limit
The amount of disk space assigned to a new box. Boxes can range in size from 4 to 1024 Mbytes.

Time Limit
The period a temporary box is available. Periods range from 30 minutes up to 12 hours.

© 2006 Critical Links, SA

Max
The maximum number of Boxes that can be active at a given time. Up to 20 Boxes may be active at one time.

3.2.6.6 USB Printers

The edgeBOX has 4 USB ports that can be used to connect printers that can be shared on the network.

Note: In order to be able to share a printer the Samba service must be running.

Connected
Displays a list of the printers currently plugged into the edgeBOX. Before a printer can be shared it must be configured. Select a printer and click on the Add button to add it to the list of configured printers.

Configured
Displays a list of the printers currently shared over the network.

To remove a printer from the network, select it from the list and click the Remove button.

© 2006 Critical Links, SA

3.2.7 Web Filtering

The edgeBOX provides a web page filtering service that can be used to block access to web sites. Filtering can be performed on either domain names or by checking URLs for certain keywords.

© 2006 Critical Links, SA

3.2.7.1 Domains

Displays a list of the web sites that are currently blocked.

Enable

Check this box to enable web filtering based on the domain name of the web site.

Add, Edit, Delete, Delete All

These buttons are used to edit the list of domain names currently filtered.

When adding a new domain, the following rules apply:

A single domain will match all urls under that domain. As an example, if you specify 'example.com', it will match 'example.com' and 'example.com/test'.

A domain preceeded by a dot will match that domain and all subdomains. For example '.example.com' will match 'example.com' as well as 'new.example.com' or 'old.example.com'.

Add from file...

A list of domain names can be stored in an external text file and loaded into the list in a single step. Clicking on this button displays a file dialog panel which allows you to locate the file on the local file system where the browser is being displayed.

© 2006 Critical Links, SA

3.2.7.2 Words in URL

Displays a list of words are used to determine whether access to a web page should be blocked.

Enable
Check this box to enable web filtering based on a specific word in a URL.

Add, Edit, Delete, Delete All
These buttons are used to edit the list of words currently filtered.

Add from file...
A list of words can be stored in an external text file and loaded into the list in a single step. Clicking on this button displays a file dialog panel which allows you to locate the file on the local file system where the browser is being displayed.

3.2.8 VoIP

edgeBOX integrates the Asterisk IP PBX to deliver a comprehensive Internet telephony solution. Its virtual PBX allows for the integration of ordinary VoIP extensions with analogue or digital (ISDN) phone lines.

The VoIP configuration options are divided into six main categories which are not completely independent:

- Phones,
- Incoming Calls,
- Outbound Calls,
- PBX Features,
- Hardware and
- Generic.

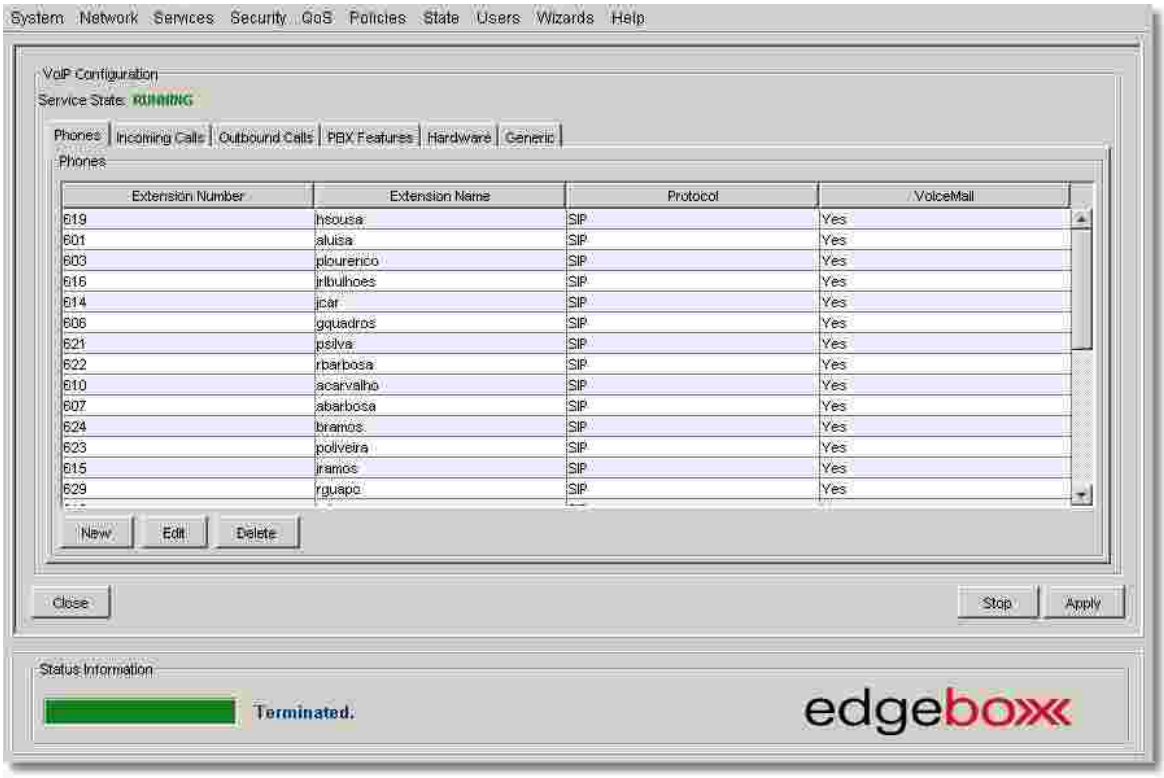
3.2.8.1 Phones

A phone is a VoIP client using one of the supported VoIP protocols: SIP or IAX. It may be a physical phone or a softphone, ie a telephony application (you can check a list of softphones at http://www.voip-info.org/wiki-VOIP+Phones#SoftPhones). After phones have been added to the system and associated with an extension, all VoIP clients need to register with edgeBOX to use the services it provides.

In this panel, the list of phones and extensions known to the system is displayed in a table. Available operations are:

- New,
- Edit and
- Delete.

© 2006 Critical Links, SA



3.2.8.1.1 New

Allows you to add a phone to the system and associate it with an extension. Four panels are available for configuration:

- § Basic,
- § Advanced,
- § Codecs and
- § Privacy.

The first panel contains basic options and its configuration is mandatory. All other panels contain advanced options for experienced users. If left unchanged, these panels will be filled with default configurations appropriate for most applications.

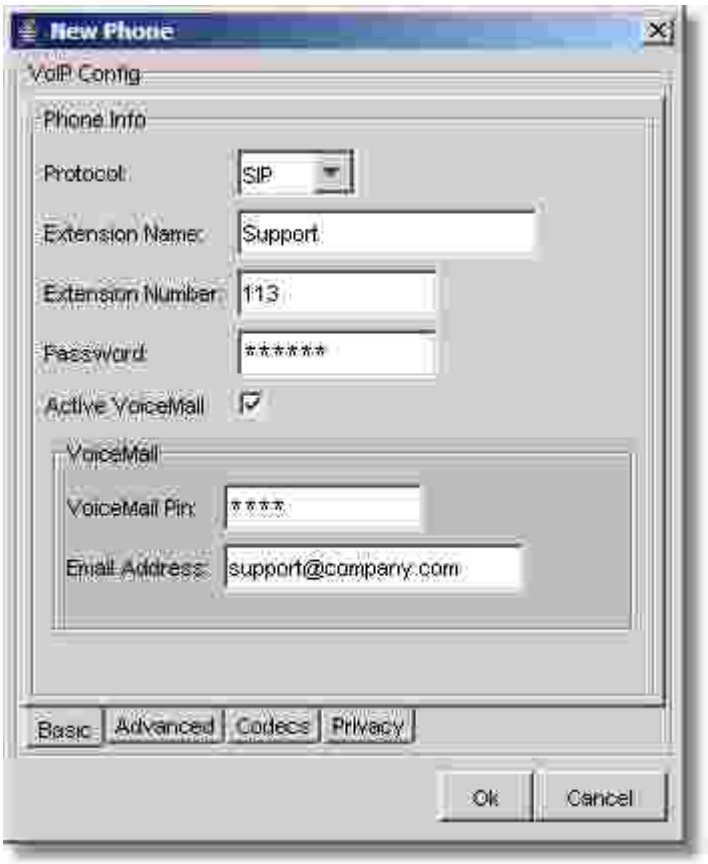
3.2.8.1.1.1 Basic

The configuration options available in this panel are:

- § Protocol: The protocol to be used by the phone. Possible choices are SIP or IAX2.
- § Extension Name: This will be the name used by the client when registering the phone with edgeBOX.
- § Extension Number: The number to be assigned to the new extension.
- § Password: Password to be used when registering this phone with edgeBOX.
- § Voicemail: If you check "Active VoiceMail", you will need to enter a pin which the user will have to supply to access this mailbox. Additionally you will also need to supply an

© 2006 Critical Links, SA

email address where the new voice mail notifications will be sent.



3.2.8.1.1.2 Advanced

This panel allows you to configure protocol-specific settings. Available options are:

§ CallerID: the name by which calls will be identified to the called party. Usually identifies

© 2006 Critical Links, SA

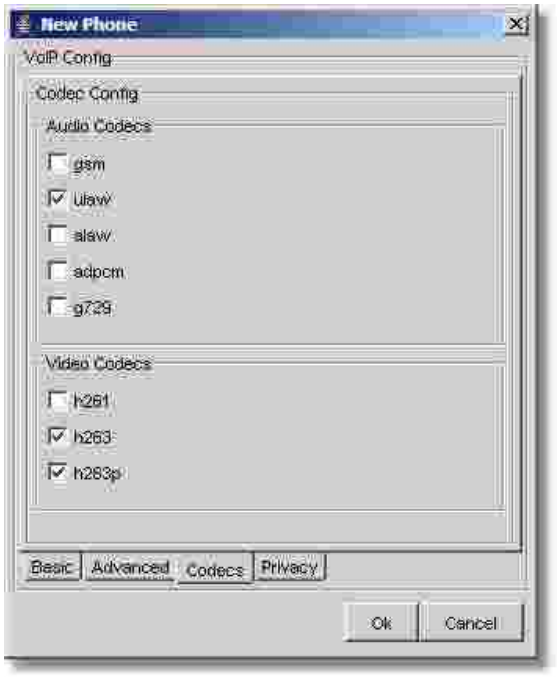
the person using the extension and their number. If left blank, a default CallerID will be generated using the data introduced previously in the basic configuration panel.

- NAT: this option should be checked when the client is behind a network address translation device such as a router or a firewall.
- MD5 (SIP only): the password used when registering the client, encrypted by an MD5 hash.
- Type: type of client using this extension. Possible values are:
  - Friend: This extension will be able to place and receive calls.
  - User: this extension will only be able to place calls.
- Host: available values are:
  - Static: If selected, you will need to specify the IP address for the client registering with the credentials entered, using the Hostname text box.
  - Dynamic (default): The client will provide its IP address when registering with edgeBOX.
- Default IP: This option will be available if you've selected "Dynamic" in the previous option. The default value is unchecked. If you check this option you will need to supply an IP address which will be used by edgeBOX to try to communicate with the client, if it hasn't registered yet.
- Port: port where edgeBOX will accept connections. Default ports are 5060 (SIP) and 4059 (IAX2).
- DTMF Mode: the way the client deals with DTMF signaling. This parameter should be consistent with the client configuration. Available options are:
  - Inband: DTMF signaling within the call. Note that this type of signaling is not supported by the GSM codec.
  - rfc2833
  - Info
- Can Reinvite (SIP Only): When active for some time, a call may be turned into a direct connection between endpoints so edgeBOX will not be in the communication path. If this is not the desired behaviour then this option should be unchecked.
- NoTransfer (IAX2 Only): Similar to the previous option. When active, all calls are routed through edgeBOX avoiding a direct connection between clients.

3.2.8.1.1.3 Codecs

Codecs are used when converting an analogue voice signal to a digital one. edgeBOX supports several types of codecs allowing a flexible client configuration. The choice of the codec to be used usually results from a compromise between sound quality and bandwidth used. Available codecs are:

© 2006 Critical Links, SA



- GSM: Usually used on European mobile networks, this codec uses a small amount of bandwidth providing an acceptable quality of sound.
- ULAW (G.711): Known as the native codec in modern communication lines. Provides good quality sound, at the expense of bandwidth. It is the most commonly used codec for VoIP calls because, besides being supported by most VoIP providers, it has the lowest latency as no type of compression is used. It is the codec used in PSTN and ISDN lines.
- ALAW (G.711): Basically, a G.711 version used in E1 European lines.

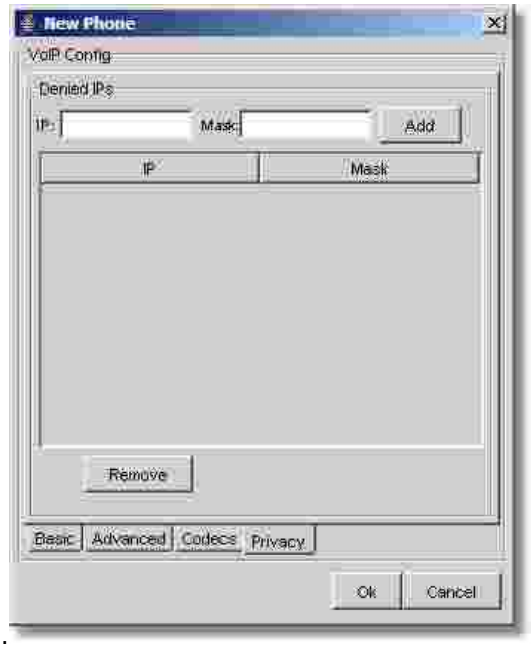
If there isn't a specific system requirement, the choice should be ULAW, because it is compatible with most phones and softphones available on the market.

- ADPCM: This is a legacy codec, kept for compatibility with version 3 of edgeBOX.
- G.729: Offers good sound quality with conservative use of bandwidth. However, to be able to use it a license must be acquired.
- H26*: These codecs are used for video calls.

3.2.8.1.1.4 Privacy

In this panel you may enter a set of IP addresses from where users will not be able to register with this phone's credentials, allowing for better control by the administrator.

© 2006 Critical Links, SA



.

3.2.8.1.2 Edit

Allows you to modify details for existing phones. All fields may be changed, except the extension name.

3.2.8.1.3 Delete

Allows you to delete a phone. There will be times when you will not be able to perform this action. Specifically when:

- This extension is used in a context (for example in a Dial action. For more information, check IVR Editor);
- This extension is used in an incoming rule (for more information, check Call Rules);
- This extension's voicemail is used in an action.

If you try to delete a phone which meets one of these conditions, a pop-up window will be displayed warning you.

3.2.8.2 Incoming Calls

This panel allows you to configure incoming call functionality, for example for calls originating from the PSTN network or internal calls between phones registered with edgeBOX. Several options are available for configuration, namely:

- IVR Editor,
- Internal,
- Call Rules,
- DID Routes and
- Sound Manager.

You access each of this panels selecting the appropriate tab on the right.

© 2006 Critical Links, SA

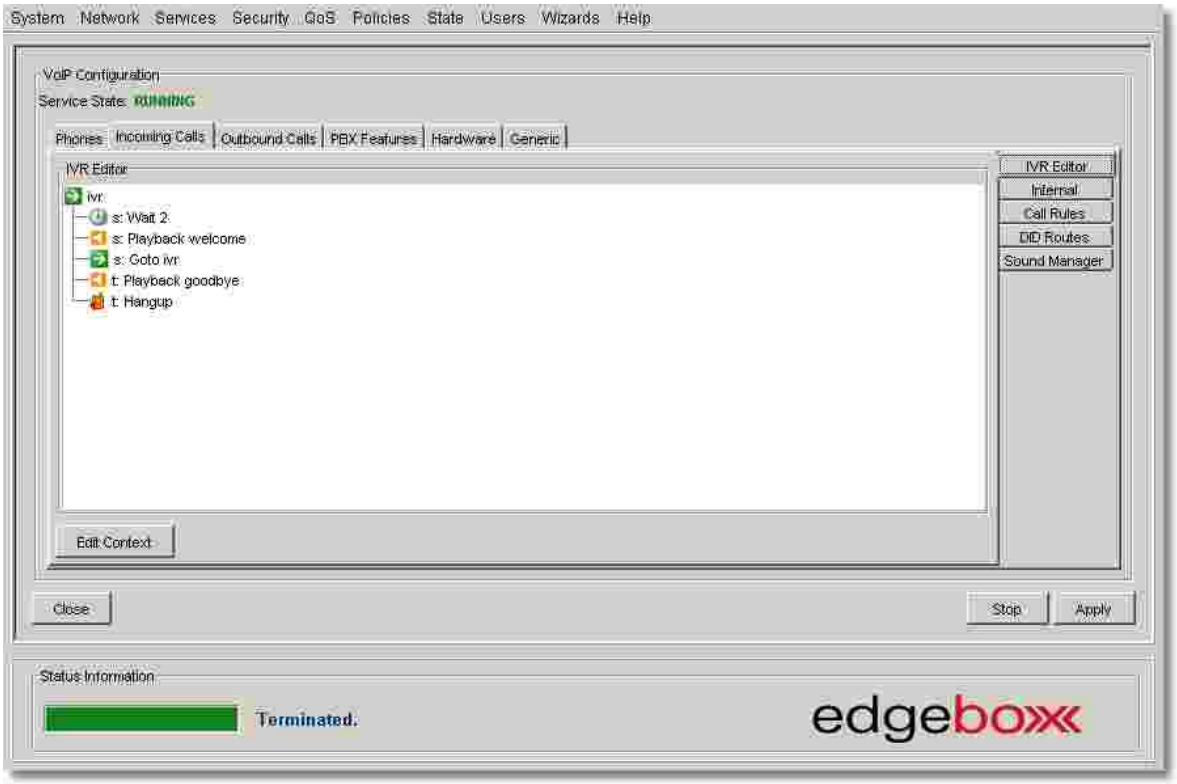
3.2.8.2.1 IVR Editor

edgeBOX provides a flexible IVR system, fully integrating all of edgeBOX's VoIP PBX functionalities, allowing the administrator to create response menus for a large range of applications. Callers using a touch tone phone will be able to navigate these menus by pressing the appropriate numbers.

An IVR system is made of contexts. Each context can have several actions, which in turn may trigger events, such as creating conferences, queues or connecting to another context, thus resulting in a navigation flow between different contexts.

The IVR system was implemented as a tree structure (see picture bellow), making it easy to understand the concept of navigating through the contexts. Each child node is either an action or a new context which may be expanded or minimised.

To add new actions to a context, select its icon and press "Edit Context" or, alternatively, double-click its icon.



3.2.8.2.1.1 Edit Context

This panel allows you to modify a particular context. After selecting the desired trigger on the left panel, its list of actions will be visible on the panel on the right. Specifically, you will be able to:

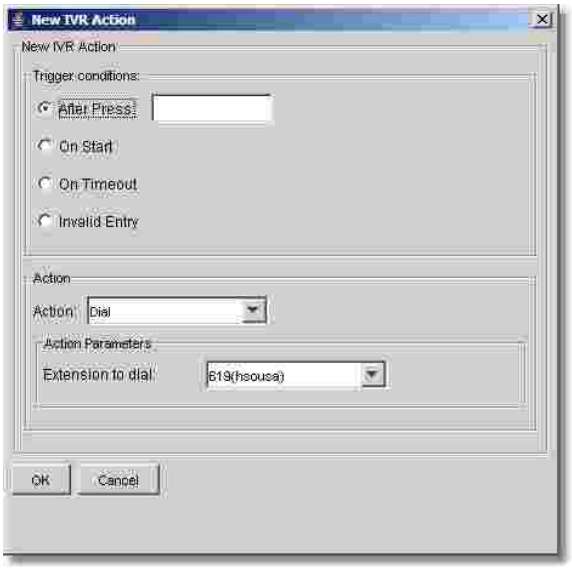
- Add new actions, by pressing the button "Add Action". A popup window will appear, requiring you to enter the action's details.
- Remove actions, by pressing the button "Remove Action", after selecting the desired action and
- Modify an action's priority, selecting the desired action and using the up/down buttons on the right.

© 2006 Critical Links, SA

This window allows you to add a new action to a context. First, you will need to define which event will trigger this action. There are four different types of triggers:

- After Press: a sequence entered by the caller.
- On Start: this action will be automatically triggered when a context is called.
- Timeout: this action will be triggered if there was no input from the caller 30 seconds after this context was called.
- Invalid: this action is fired if the caller inputs a sequence with no action assigned to it in the context.

© 2006 Critical Links, SA

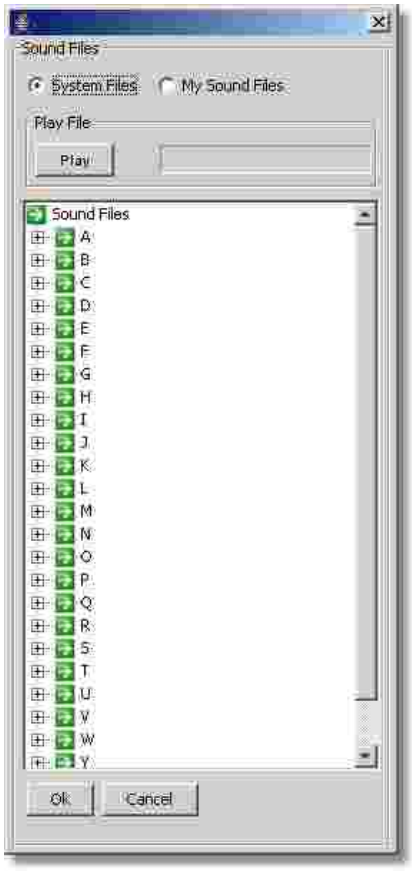


The following action types are available:

- Dial: a call will be placed for the chosen extension. You may choose any extension previously configured using the phones' panel, as well as any FXS mode analogue ports or any NT mode digital ports, available in BRI cards.
- Voicemail: the call will be forwarded to the chosen extension's voicemail. You may choose any extension with an active voicemail.
- Goto: The call will be routed to another context. For more details, check Goto Action.
- Hangup: this action will terminate the call.
- Wait: a pause is introduced in the call. You will need to specify the number of seconds this pause will last.
- Queue: the call will be forwarded to a queue. You may choose any queue previously configured in the system.
- MeetMe: this call will join a conference. You may choose any static conference previously configured in the system.
- HuntGroup: all phones associated with the selected huntgroup will ring. The call will be forwarded to the first one to answer. You may choose any hunt group previously configured in the system.
- PlayBack: the selected sound file will be played and all numbers entered by the caller will be ignored.
- Background: the selected sound file will be played but this time all numbers entered by the caller will be processed, and resulting actions will be performed.

To select a sound file, press the "Select Sound File" button. A new popup window will display, allowing you to choose the sound file either from "System Files", or from "My Sound Files" (files uploaded by the administrator).
You may listen to the files, using the "Play" button. This way, you may choose the sound file most appropriate for the situation.

© 2006 Critical Links, SA



One of the most important IVR actions is the Goto action, which allows navigation between the available contexts.
After selecting this action, you need to supply the target context. This may be a previously created context or a new context.
If you want to create a new context, select the "New Context" option, and insert the new context name.

The edit context panel is divided in two main sections. On the left side it is possible to select the event that will trigger its actions. After selecting an event, its actions will be visible in the right panel. The actions are ordered by priority - with the top most being the ones executed first. The "Up" and "Down" buttons allow you to change the actions' execution order.
Remember that you will need to press the "OK" button to confirm your changes. The IVR edition panel will then be visible again, where you can check all changes made to the context.
If you've created a goto action to a new context, it is possible to select this context to edit its actions.

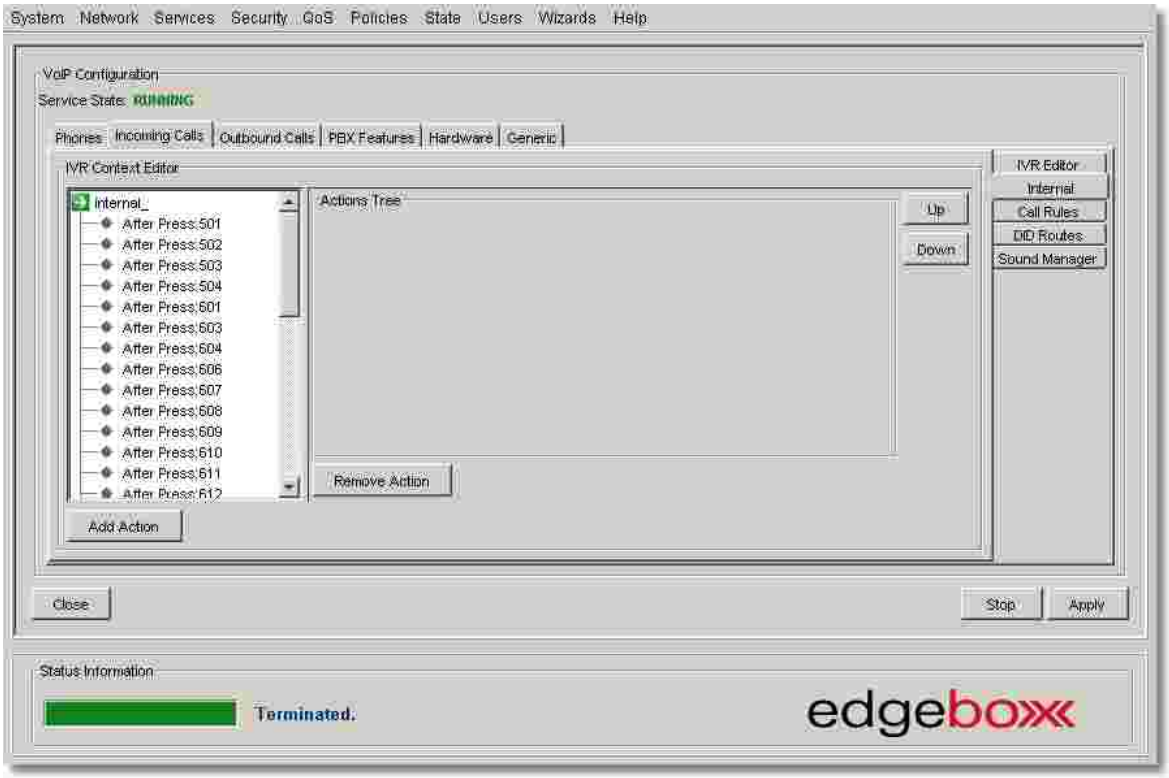
Allows you to remove an action from a context.

3.2.8.2.2 Internal

This panel allows you to configure internal extension routes. By default, a route is created at phone creation time when you supply an extension number. These routes may be completely changed, though.

This panel is similar to the IVR's context edition panel. The extensions are shown on the left panel and its actions are shown on the right side.

© 2006 Critical Links, SA



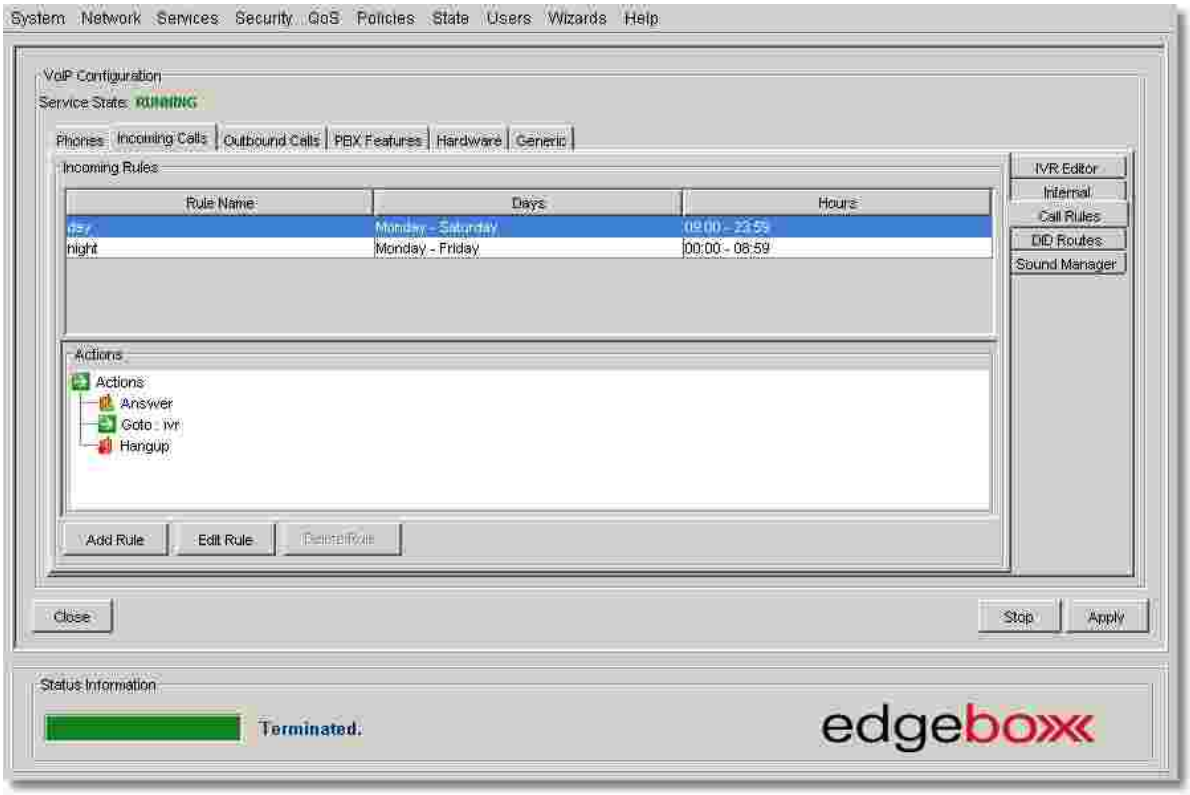
3.2.8.2.2.1 Add Action

The options presented in this panel are the same as the ones in the IVR editor's Add Action.

3.2.8.2.3 Call Rules

edgeBOX allows you to define rules to deal with incoming calls according to the hour/day in which they arrive. This way the administrator may define different actions depending on the hour of the day. For example, it is possible to play a message warning the company is closed during evening hours. It is also possible to define special rules for weekends and holidays.
At least one rule needs to be defined for incoming calls. To define a new rule, select the "Add Rule" button. Rules can also be modified, using the "Edit Rule" button, and removed using the "Delete Rule" button.

© 2006 Critical Links, SA



3.2.8.2.3.1 Add Rule

This panel allows you to create a call rule. For each rule definition, the time frame to which it applies and the actions to be executed have to be defined.

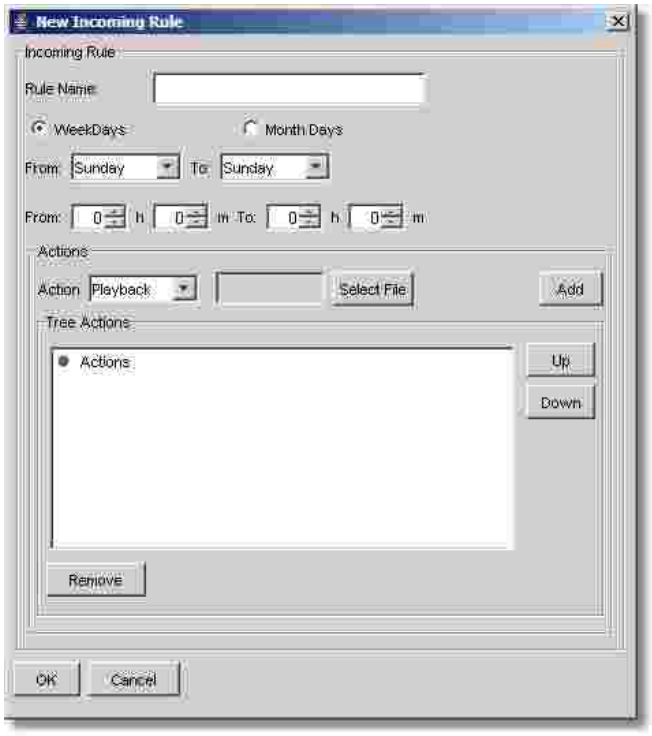
Time frame:

- Weekdays: If you select this option, you will need to select the weekdays between which this rule will be applied. For example, if we want to define a rule to be applied during the weekend, the limits should be defined as Saturday and Sunday.
- Month Days: If you select this option, you will need to select the month days between which this rule will be applied. Use this option when you want to define a rule to be applied to an holiday.
- Hours: Regardless of the option selected for days (Weekdays or Month Days), you will also need to select the hours interval to which this rule will be applied. If you want the rule to be valid for a whole day, this interval should be defined from 00:00 to 23:59.

Actions:

At least one action should be defined for each rule. The actions available here are exactly the same as when modifying a context in the IVR panel. In the same way, the actions have an execution order, which may be changed using the "Up" and "Down" buttons.
Using the Goto action, the call may be forwarded to any context defined in the IVR. Bear in mind that for a call to enter the IVR flow, there should be an explicit rule here directing it to the IVR (using a Goto action to the IVR context).

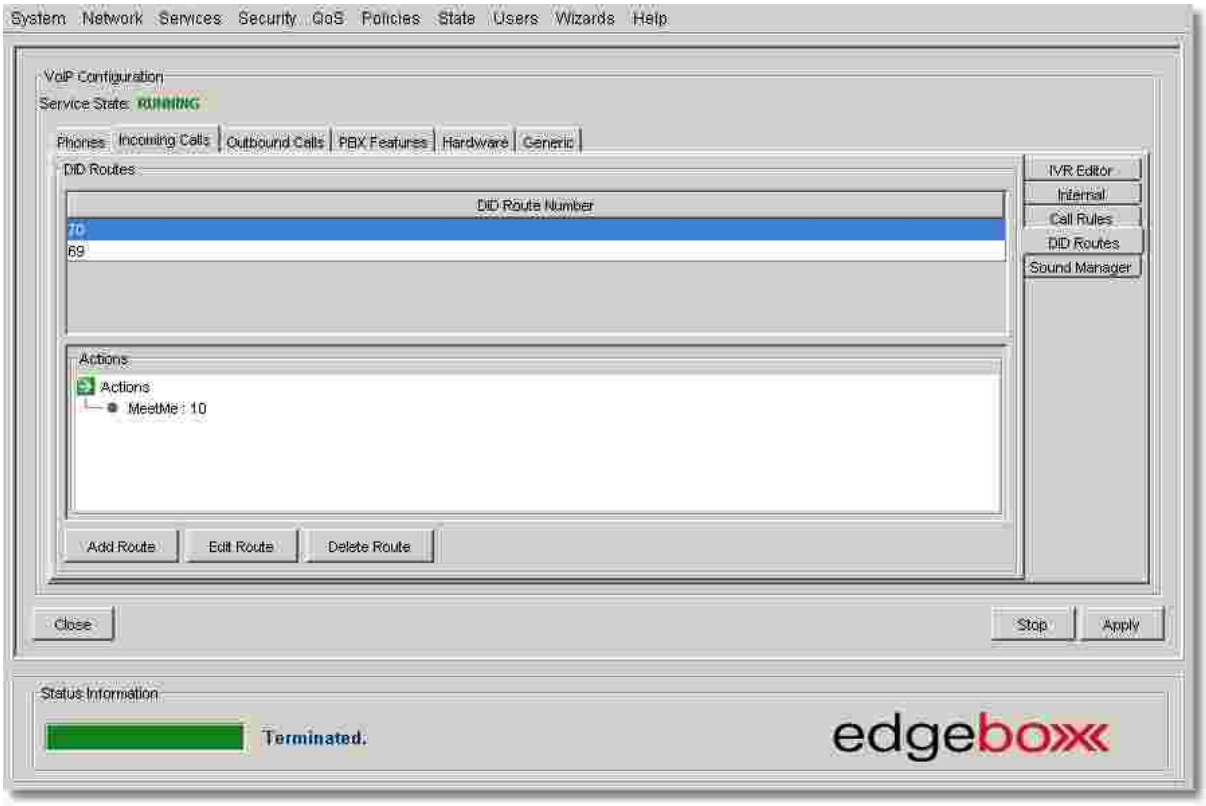
© 2006 Critical Links, SA



3.2.8.2.4 DID Routes

Using DID routes, it is possible to define rules for specific incoming call numbers. This functionality may be used when you wish to have a set of actions assigned to a specific number, for example to allow an internal extension to be accessed from outside directly.
You may add a new DID route, selecting the "Add Route" button, modify a DID route, using the "Edit Route" button or remove a route, selecting the "Delete Route" button.
Please note that for DID routes to work, we assume that hardware capable of performing incoming number recognition is installed in edgeBOX. For that to happen, a BRI or PRI card must be connected to a digital line.

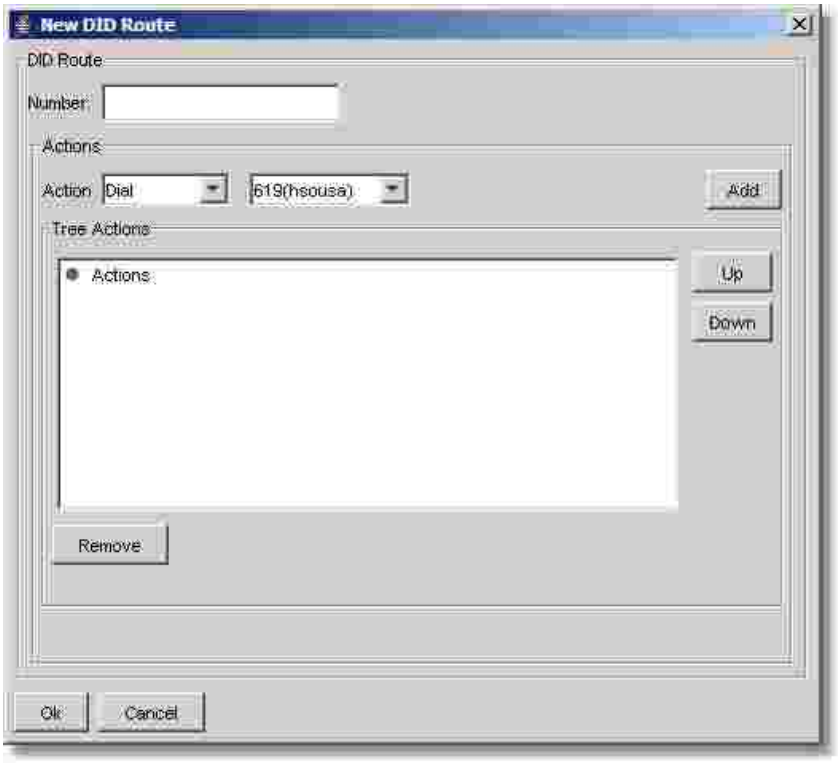
© 2006 Critical Links, SA



3.2.8.2.4.1 Add Route

To define a DID route, enter the number and define the set of actions to execute. The set of actions available are the same ones available in the Add Action popup windows in the IVR context editor.

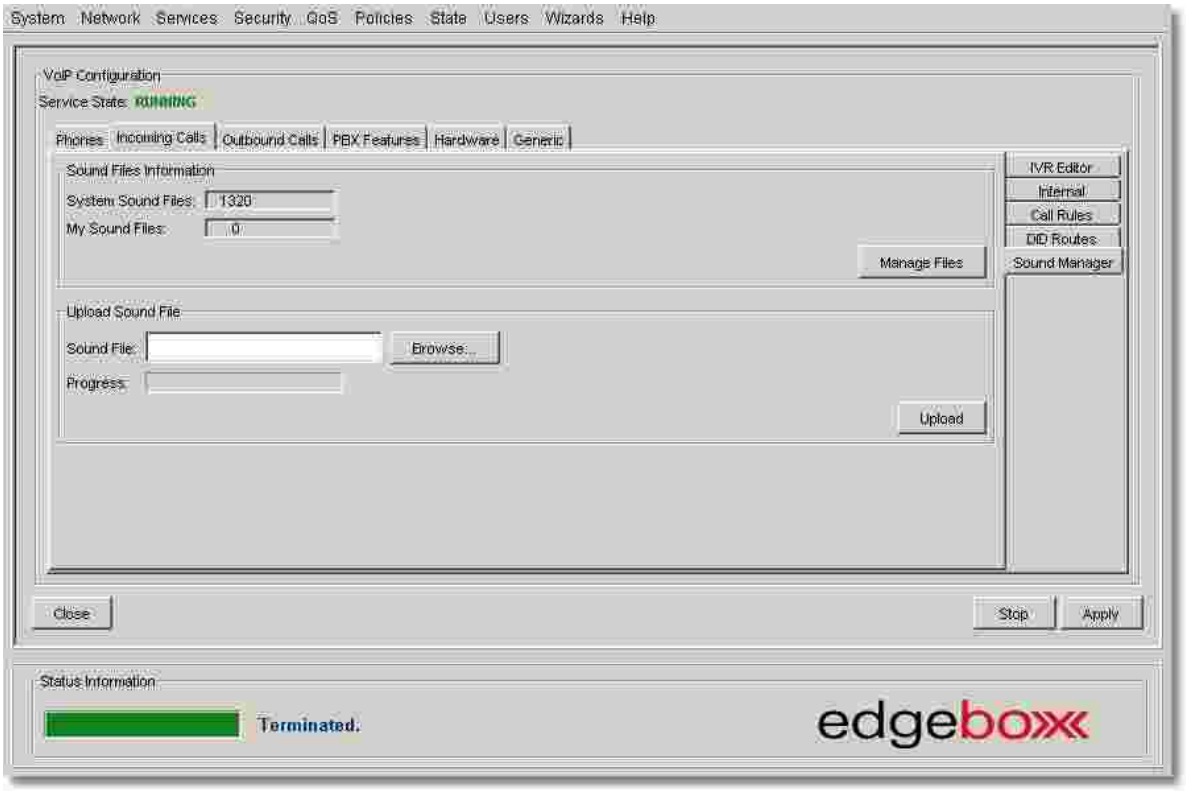
© 2006 Critical Links, SA



3.2.8.2.5 Sound Manager

In order to use the "Playback" and "Background" actions, you need to select the sound file to use. This file may be a system file or a user file. This panel allows you to upload ".gsm" sound files. Select the desired file using the "Browser" button, and then select the "Upload" button.
If this operation is successful, the uploaded file should be available in the sound files management panel, where files may be played or deleted

© 2006 Critical Links, SA



3.2.8.3 Outbound Calls

This panel allows you to configure several aspects related with outgoing calls. An outgoing call needs a route to be configured. There are two different kinds of outgoing routes:

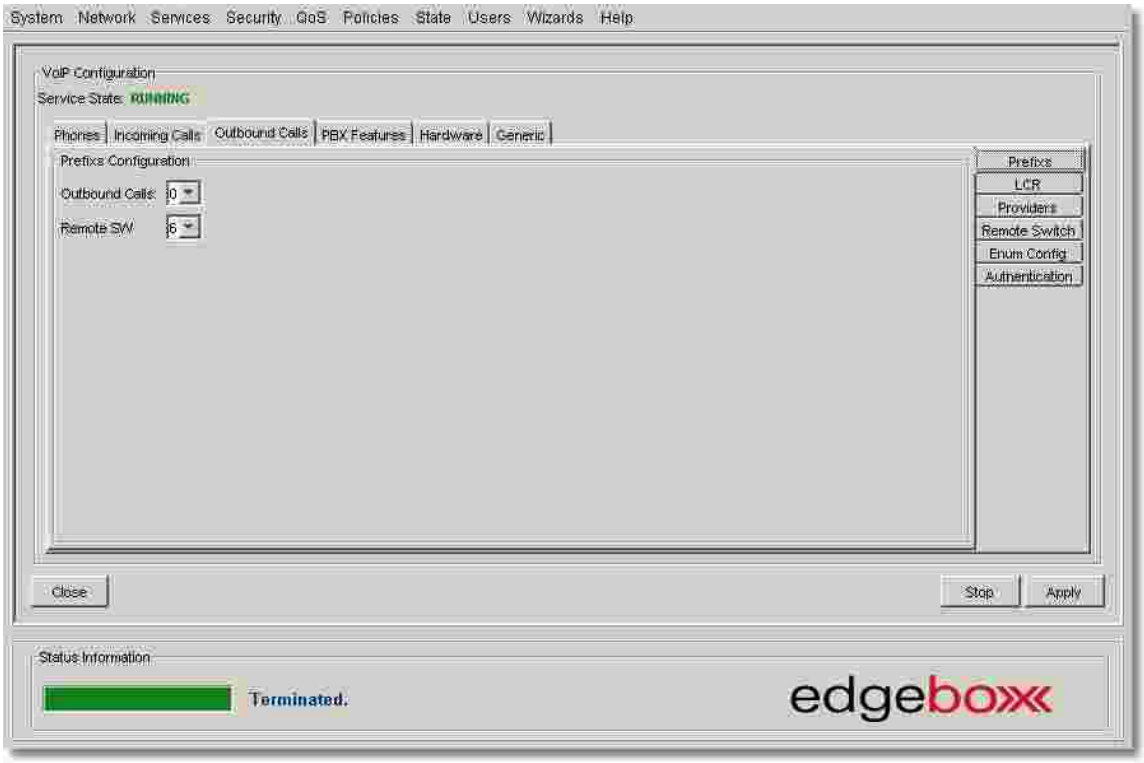
- Direct connection to the PSTN network, using hardware installed on edgeBOX and
- a VoIP Provider properly configured.

3.2.8.3.1 Prefixes

In order to discriminate the type of calls that can be placed, a prefix needs to be configured. There are different types of calls which will need a prefix:

- Outgoing calls using predefined routes and
- Calls to extensions belonging to another edgeBOX (Remote Switch).

© 2006 Critical Links, SA



3.2.8.3.2 LCR

Outbound calls (identified by the appropriate prefix) can be divided into five different groups:

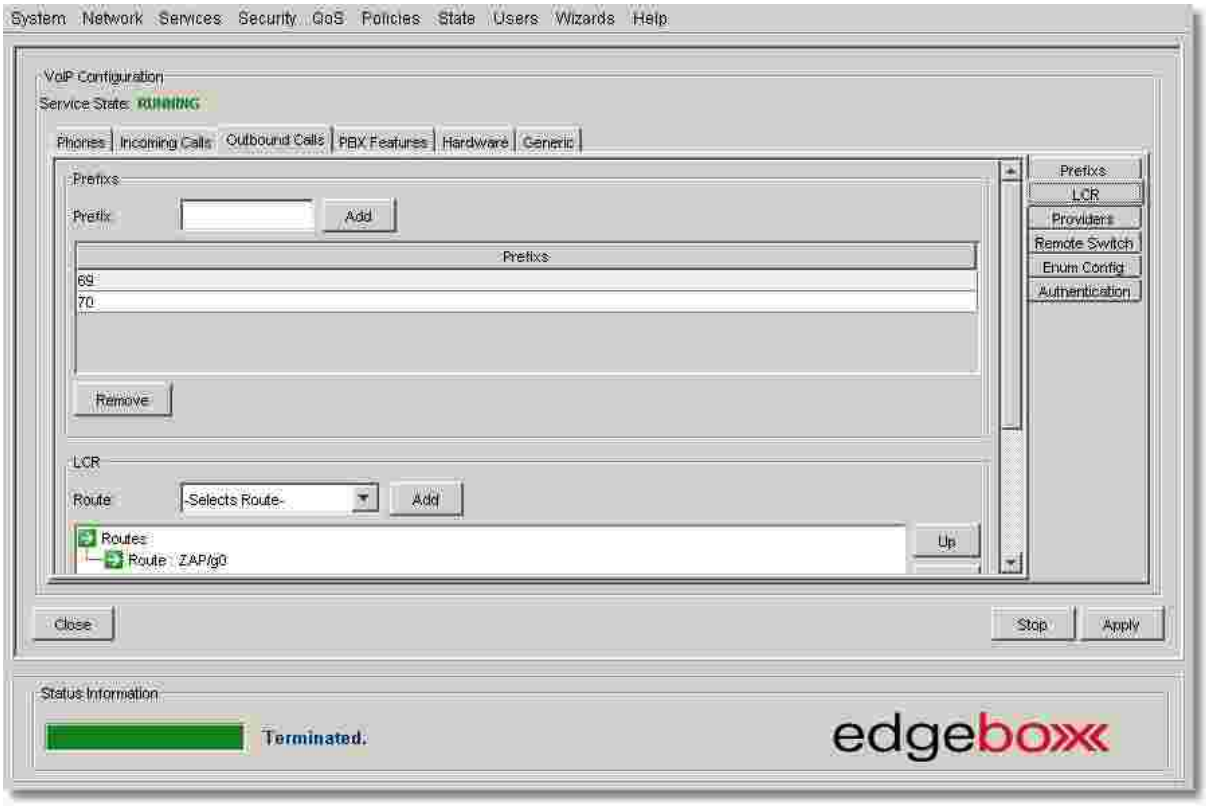
- Local calls,
- Long distance calls,
- Mobile calls,
- International calls and
- Free Calls.

For each of these groups, you will have to configure at least a route and the prefixes that will identify the group to which the call belongs. For instance, an international call will always be preceded by the "00" prefix. This prefix will identify a call as belonging to the group of international calls. For the correct call identification to occur, all prefixes have to be added to the system - otherwise the call will fail. If a prefix is not defined in this panel, the call will be considered by default an international call.

All outbound interfaces provided by VoIP hardware installed and VoIP providers configured will be available as outbound routes. Each group may have more than one outbound route. If the call fails using one route the next route will be tried. Route priorities may me changed using the "Up" and "Down" buttons on the right side.

Besides supporting different LCR per group, the use of prefixes to identify the group the call belongs to also allows administrators to restrict the type of calls users are allowed to make. For more information, see Authentication.

© 2006 Critical Links, SA



3.2.8.3.3 Providers

edgeBOX may also work as a client for SIP/IAX servers. This panel allows you to configure edgeBOX to work this way using the services offered by VoIP providers. Currently there are several VoIP providers offering calls to local PSTN networks in several countries at very competitive prices.

© 2006 Critical Links, SA

VoIP providers configured are show in tabular form. The options available are:

- Add a new VoIP provider,
- Edit an existing VoIP provider details and
- Delete a VoIP provider.

It is possible to change the details for all VoIP providers, selecting it on the table and the pressing the "Edit" button or by double clicking on its entry. However, there may be situations where you will not be able to do so. For instance, when a VoIP provider is used in an LCR outbound route, editing is disabled to prevent possible problems in registration with remote servers. In such cases, first you will have to delete the LCR route using the provider, and only then you will be able to modify its details.

3.2.8.3.3.1 Add

Allows you to configure a VoIP provider. For edgeBOX to be able to use the services of a VoIP provider you just have to specify the necessary authentication credentials.

To make this configuration easier the VoIP provider control is filled with the most common VoIP providers:

- iaxTel
- Gossiptel
- SipGate
- IpTel
- FreeWorldDialup

© 2006 Critical Links, SA

- VoipBuster
- SipPhone

After selecting the desired provider you will need to supply a name for this provider and the necessary credentials (username and password). After pressing the "Ok" button this provider will be available to use in a LCR route.

If the desired provider is not found on the list, you can add it by using the "Custom" option and filling in the necessary fields:

- Protocol: the protocol used by the provider;
- Host: the provider's server address;
- NAT: activate if the provider is behind a router/firewall and
- Codecs: select the codecs to be used (these codecs have to be supported by the provider)

Using this option also allows you to use a SIP proxy for outbound calls.

3.2.8.3.4 Remote Switch

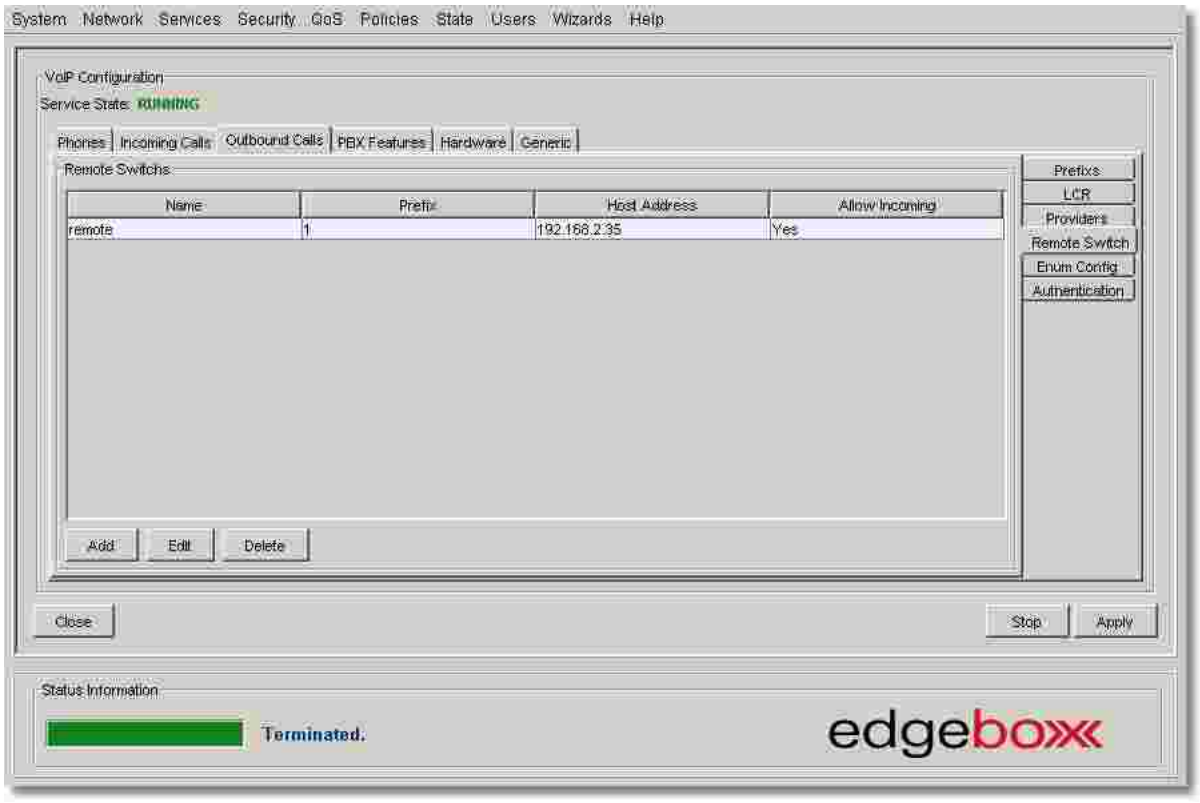
The Remote Switching functionality allows the creation of an IAX trunk between two edgeBOXs. Calls between these devices benefit from an optimised connection, resulting in a better use in bandwidth.

You can check the remote switches configured in the system which are displayed in tabular form. Options available are:

- Add, to add a remote switch configuration,

© 2006 Critical Links, SA

- Edit, to modify an existing remote switch configuration and
- Delete, to remove a remote switch configuration.


System Network Services Security QoS Policies State Users Wizards Help
VoIP Configuration
Service State: RUNNING
Phones Incoming Calls Outbound Calls PBX Features Hardware Generic
Remote Switchs
Name Prefix Host Address Allow Incoming
remote 1 192.168.2.35 Yes
Add Edit Delete
Prefixs LCR Providers Remote Switch Enum Config Authentication
Close Stop Apply
Status Information
Terminated.
edgeboxx

Another benefit from this configuration is that an extension from edgeBOX A is able to call an extension registered in edgeBOX B.

As an example, consider you are using an extention from edgeBOX A and you want to call extention 600 from edgeBOX B. First step is to define the prefix for remote switch (see Prefixes); in our example this prefix is ‘6’. Then, add a new remote switch configuration (see Add); in our example the prefix for this connection is ‘1’.

Having this configuration done, you will be able to call to the extension on edgeBOX B dialling: prefix for remote switch (6) + prefix for remote schitch connection (1) + extension number, ie, you would dial 61600.

When you add a remote switch, you are creating an one way connection, on the hostname direction. If you also want to receive calls using that trunk (which is usually the case) you will need to activate the option ‘Allow incoming calls’. Having this set, and if the remote edgeBOX also defined your edgeBOX as a remote switch with the **same name** a two ways trunk will be created, allowing

© 2006 Critical Links, SA

incoming and outgoing calls.

Note that besides calling internal extensions, all VoIP funcionalities will be available for the remote edgeBOX users (making local calls, making call conferences, etc.), allowing you to make a conference call between to remote offices with no costs.

3.2.8.3.4.1 Add

Allows you to add a new remote switch configuration. You must supply the following data:

- Prefix: prefix to identify this connection;
- Name: connection name;
- Secret: password used to register with the remote edgeBOX;
- Host: remote edgeBOX address;
- Codecs: codecs to be used during calls between the two edgeBOXs (local and remote).

3.2.8.3.5 Enum Config

edgeBOX supports Enum, which is a service mapping PSTN telephone numbers into VoIP URLs. If you activate Enum servers edgeBOX will send a query to each active server to try to lookup the called PSTN number. If a matching answer is received the call will use the VoIP URL returned and so transparently divert to the Internet, having no cost. Otherwise, the call will follow the route configured in the LCR.

© 2006 Critical Links, SA

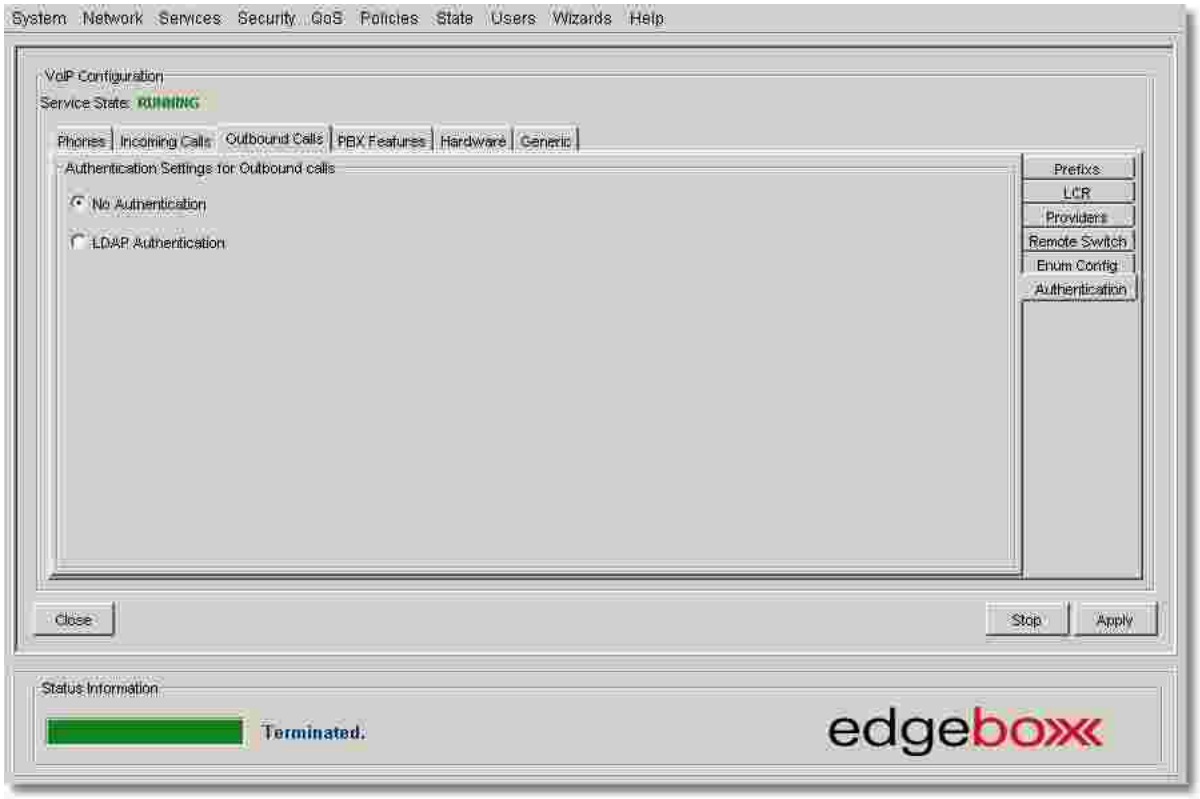
3.2.8.3.6 Authentication

edgeBOX supports authentication for outbound calls. Authentication is based on a PIN number, which is assigned on user creation (see Users in User and Group Management). Outbound call permissions, i.e. the type of outbound calls a user is allowed to make, are also set on user creation.

This panel allows you to activate VoIP authentication. The system will block outbound calls if the user supplied invalid credentials or if the user doesn't have the necessary permissions to make the call.

If authentication is not active, the system will still check the type of each call but just to find the best LCR to use. In this mode of operation users are not required to supply a PIN when making calls.

© 2006 Critical Links, SA



3.2.8.4 PBX Features

This section describes edgeBOX's IP PBX advanced features. All these features can be used in the IVR editor, making them available to calls coming from the external network.

The following features will be described:

- Queues,
- Agents,
- Conferences,
- Parking,
- Huntgroups and
- Voicemail

3.2.8.4.1 Manage Queues

This panel allows you to manage edgeBOX's queuing system. These services are widely used, especially in Call Centres where callers are usually placed in a queue before an operator answers the call. Configured queues are shown in a tabular manner. You can create new queues ("Add Queue" button), modify existing queues' details ("Edit Queue" button) or remove a queue ("Delete Queue") button.

© 2006 Critical Links, SA

3.2.8.4.1.1 Add Queue

Allows you to create a new queue.

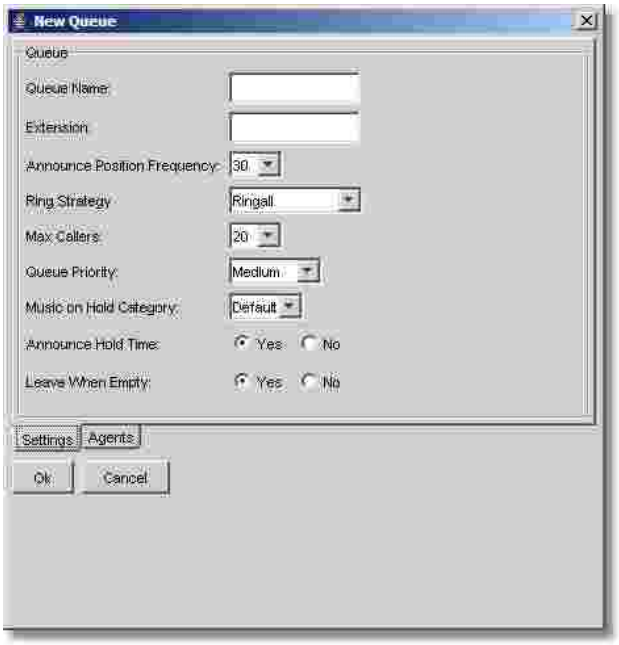
Settings

General queue settings are configured selecting the "settings" tab page. Available options are:

- Queue Name: name assigned to this queue;
- Extension: internal extension associated with this queue;
- Announce Position Frequency: time interval (in seconds) between queue position announcements;
- Ring Strategy: algorithm used to assign calls to agents:
  - RingAll: all agent phones will ring, and the call will be assigned to the one that answers first;
  - RoundRobin: selects each agent in turn;
  - LeastRecent: selects the agent which was least recently selected;
  - FewestCalls: selects the agent with least calls answered;
  - Random: selects an agent randomly;
  - RR with Memory: RoundRobin with memory, remembers which agent answered last and selects the next one.
- Max Callers: maximum number of calls that can be placed on this queue;
- Queue Priority: queue's relative priority to other queues configured;
- Music on Hold: music that will be played when the call is queued;

© 2006 Critical Links, SA

- Announce Hold Time: set to Yes if you want queue position to be announced, set to No otherwise;
- Leave When Empty: set to Yes if you want calls queued to be terminated if there are no agents assigned to the queue.



Agents

For a queue to work correctly agents must by assigned to it, since queued calls are answered by agents.
To associate an agent with a queue select the "Agents" tab page. The agents assigned to this queue are displayed in a tabular manner.
To associate an agent with a queue select the desired agent in the agents' list, and the press the "Add" button. To remove an existing association, select it on the table and press "Remove". Note that for having an agent available on the agents' list it must have been previously created using the Agents panel.

© 2006 Critical Links, SA

3.2.8.4.2 Agents

This panel allows you to manage agents that will later be associated with queues, and configure general agent settings.
Essentially, there are two different strategies for agents: either the agent logs on and remains logged on until an inbound call is assigned, or an agent logs on and then logs off and gets called in the event of an inbound call.

Agent Settings

Callback Login

If you enable this option agents will be called when an inbound call arrives. You will need to supply an extension that will be used by the agents to log on. The agents will call this extension, and after entering their agent ids and pin numbers, they will be ready to answer calls from queues they are associated with.

Other options available are:

- Auto LogOff Time: time, in seconds, after which the agent will be logged off from the system if the call is not answered;
- Require Ack: if set to "Yes", the agent will have to press "#" to accept an incoming call;
- Music on Hold: music the agent will listen to while waiting a new incoming call.

Agents

Configured agents are displayed in a tabular manner. You may create new agents (selecting the "Add agent button"), modify an agent settings (selecting the "Edit Agent" button or double clicking the desired agent) or remove an agent (selecting the "Delete Agent" button).

© 2006 Critical Links, SA

3.2.8.4.2.1 Add Agent

Allows you to create a new agent. You will need to supply the following elements:

- Agent ID: number identifying this agent;
- PIN: PIN number the agent will use to authenticate;
- Agent Name: name for this agent;
- Login Extension: extension this agent will use to register in a queue. If this method is used, the phone must remain off-hook (online).

3.2.8.4.3 Conferences

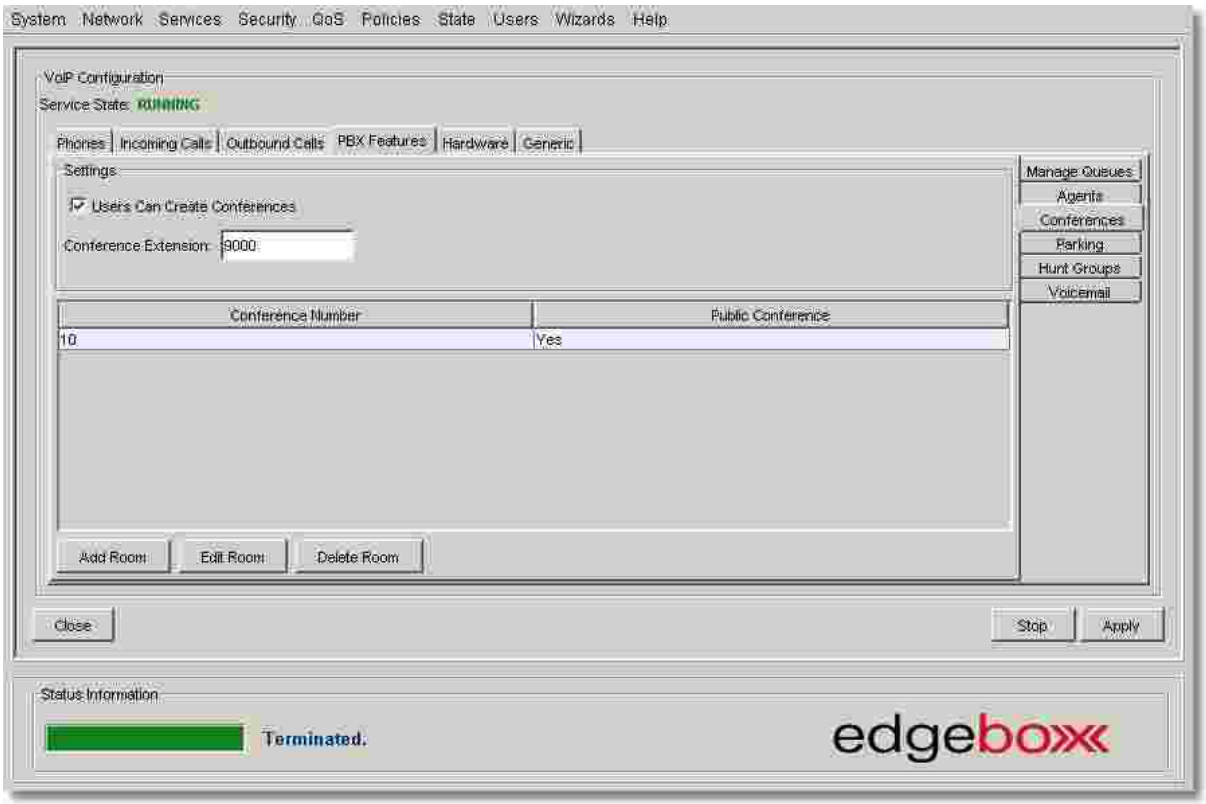
edgeBOX supports two types of conferences:

© 2006 Critical Links, SA

- Dynamic conferences and
- Static conferences.

To activate dynamic conferences, check the "Users can Create Conferences" option. You will also need to supply an extension for this purpose (by default, it is "9000"). In this type of conference, any registered user may dial the pre-defined extension and create a conference by pressing a number. To join this conference, users just have to dial the pre-defined dynamic conferences' extension ("9000" in our example) and enter the conference number.

Static conferences have to be created beforehand by the administrator. The list of static conferences configured is displayed in this panel in a tabular form. You may create a new static conference (by pressing the "Add Room" button), modify a static conference's details (pressing the "Edit Room" button) and remove a static conference ("Delete Room" button).



3.2.8.4.3.1 Add Room

Allows you to create a new static conference. The following elements must be supplied:

- Conference Number: internal extension assigned to this conference;
- Protected Conference: If you enable this option, you will need to supply a conference PIN and an administrator PIN. Users will then have to enter the correct PIN to join this conference.

All configured static conferences can be used when you use the IVR editor to add a MeetMe action.

© 2006 Critical Links, SA

3.2.8.4.4 Parking

The parking call service is ideal for transferring calls. To configure this service, you will have to supply the following elements:

- Number to Dial: number to dial to place the call on hold;
- Number of Lines: number of extensions available for parking and
- Parking Max Time: the maximum amount of time a call can remain on hold.

To park a call, dial "#" plus the number configured in the "Number to Dial" field. A message will inform you in which extension the call was parked into (let's assume it was 701). This call can then be answered from any internal extension dialing 701.

© 2006 Critical Links, SA

3.2.8.4.5 Hunt Groups

With this service, you can create a group of phones so that when a call arrives for the group, all phones in that group will ring at the same time. The first one to answer will keep the call. Configured huntgroups are displayed in a tabular form. You may create a new huntgroup ("Add HuntGroup" button), change a huntgroup's configuration ("Edit HuntGroup" button) or Remove a huntgroup ("Delete HuntGroup").

© 2006 Critical Links, SA

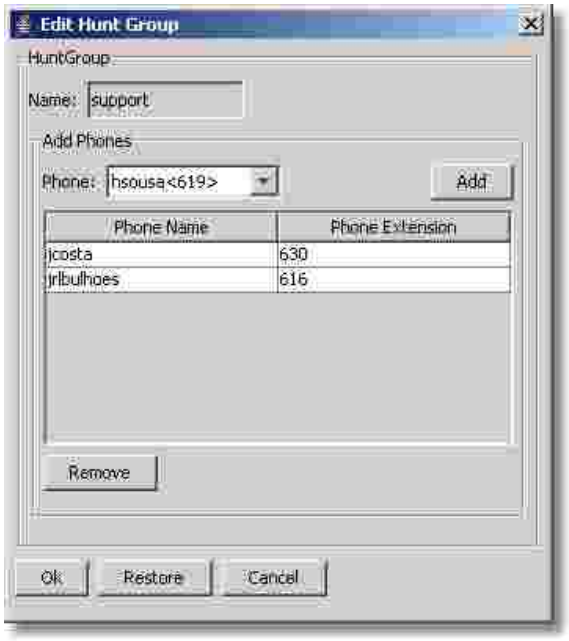
3.2.8.4.5.1 Add HuntGroup

This option allows you to create a new huntgroup. You will need to supply the following information:

- Name: the name for this huntgroup and
- Phones: the phones associated with the huntgroup. After selecting the desired extension press the "Add" button to add the phone to the huntgroup.

When configuring the IVR system, remember that all huntgroups configured may be used in the action "HuntGroup".

© 2006 Critical Links, SA



3.2.8.4.6 Voicemail

In the voicemail configuration panel you can define some of its functional parameters.

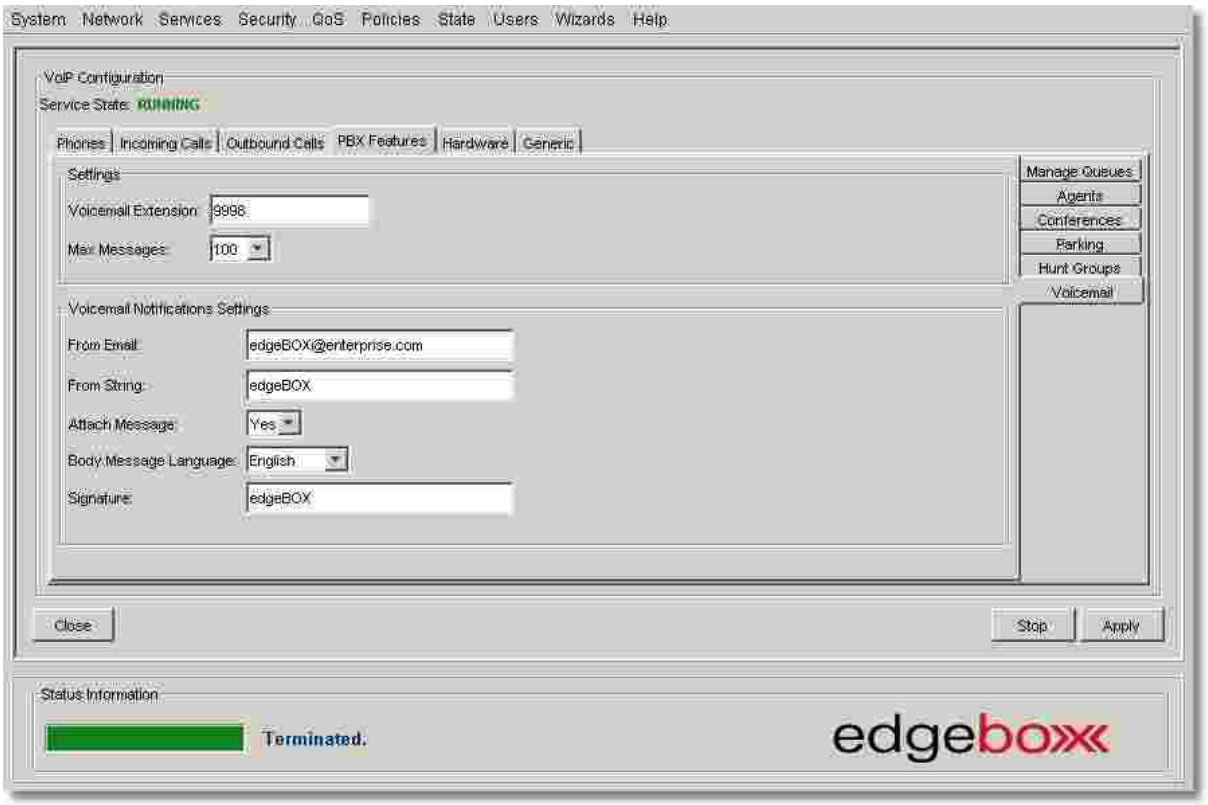
In general settings you can define:

- Voicemail Extension: extension number where you can access the voicemail system and hear your messages.
- Max Messages: maximum number of messages that a user can have in his/her mailbox.

You can also define parameters to the notification messages, ie messages edgeBOX sends when a user receives a new voicemail message:

- From Email: origin e-mail address of notification messages.
- From String: name of the entity originating notification messages.
- Attach Message: when active, the voicemail message is attached to the notification message in audio format.
- Body Message Language: language used in notification messages. There are two available options: English and Portuguese.
- Signature: signature of the notification messages.

© 2006 Critical Links, SA



3.2.8.5 Hardware

edgeBOX supports automatic hardware detection. All supported VoIP cards are detected and the system is automatically configured so these cards can be used by the IP PBX. Only information related to the card currently installed in the system will be displayed in this panel. The supported VoIP cards are:

- ISDN BRI,
- ISDN PRI and
- Analogue FXO-FXS.

3.2.8.5.1 ISDN BRI

edgeBOX supports BRI VoIP cards.

It is possible to configure global settings such as the country national prefix as well as the prefix used to make international calls. Another option available for configuration is the call volume which may vary between an 8db gain or loss. This value should be adjusted depending on the network.

All ports detected will be displayed on the table where its operation mode can be checked. Ports are initialised in TE operation mode by default.

There are two port operation modes possible:

§ TE mode: ports should be connected to ISDN lines.

© 2006 Critical Links, SA

- NT mode: ports should be connected to ISDN phones.

You may change the port working mode. To do so, select the desired port and press the "Edit Port" button. You may also double click the desired port.

3.2.8.5.1.1 Edit Port

When editing a BRI port, you can configure the port operation mode. Available values are NT or TE. This panel also allows you to supply the msns.

In TE mode, the msns will be needed in order to be able to use DID routes. In NT mode, you will need to define the msns in order to distinguish between the phones connected to the bus. The msns associated with the phones must be configured accordingly.

All ports detected as working in NT mode will be available as phones when editing the IVR and in internal extensions management. In the same way, all ports detected as working in TE mode will be available as outbound routes when editing the LCR.

Note that if you change a port operation mode the PBX will be reinitialised and all ongoing calls will be hung up.

3.2.8.5.2 ISDN PRI

One of the types of VoIP cards supported by edgeBOX is PRI Digium cards. These cards may have one, two or four spans. All spans detected will be displayed in a tabular manner, where you can also check some other span settings:

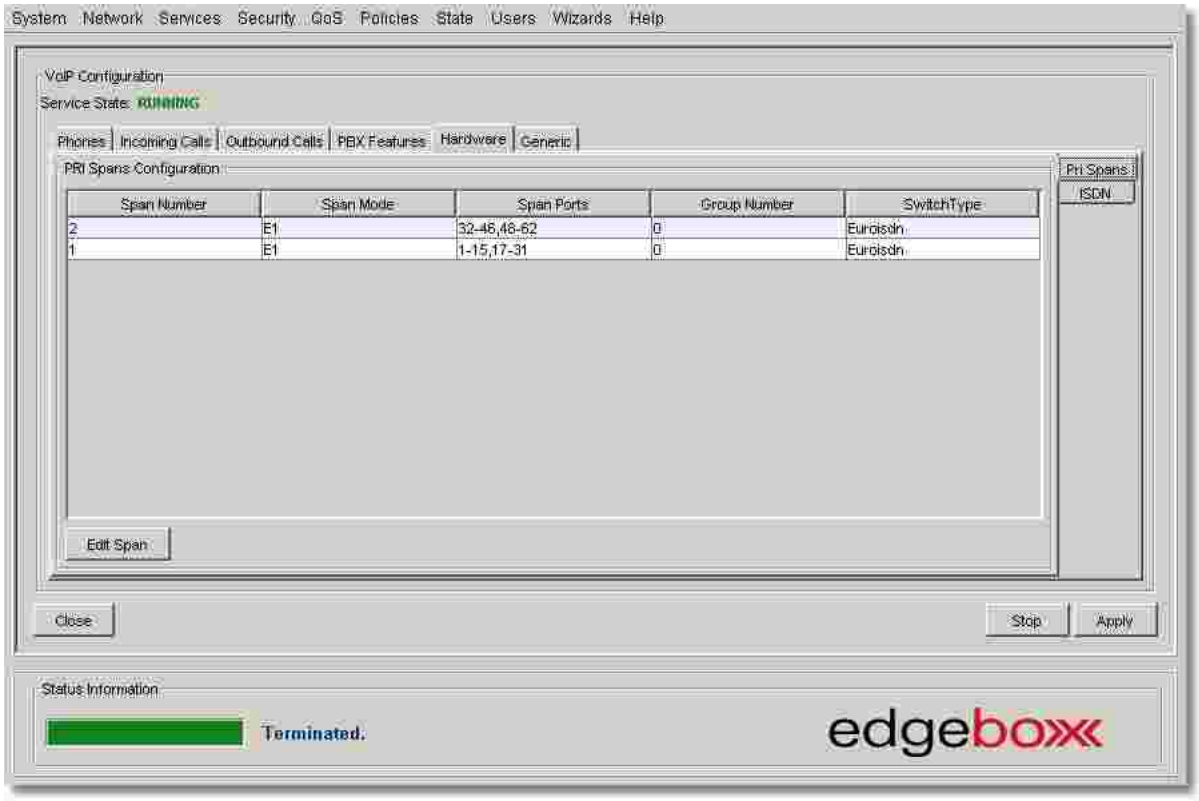
- Span Number: port number;
- Span Mode: port working mode (Available values are T1 or E1. This mode can be configured using a card jumper);
- Span Ports: number of ports associated with the span. (31 ports in E1 mode, 22 ports in

© 2006 Critical Links, SA

T1 mode);

- Group Number: group to which the span belongs to;
- SwitchType: type of span to which the line will be connected to.

Some of the span properties can be changed. To do so, select the desired span and press the "Edit Port" button. You may also double click the desired span.



3.2.8.5.2.1 Edit Port

The following settings may be changed:

- Signalling: signalling used by this span. Available options are:
  - PRI_CPE used on the client side;
  - PRI_NET used on the network side.
- SwitchType: switching used by the line. Available options are:
  - EuroISDN, used in Europe;
  - National used in the USA.
- Context: incoming calls context (by default is incoming);
- Group: group to which this span is associated to.

© 2006 Critical Links, SA

3.2.8.5.3 Analogue FXO-FXS

To allow connection to analogue lines, edgeBOX supports TDM Digium cards. FXO and FXS modules may be installed in this card:

- FXO Module: should be connected to an analogue line, allowing you to receive or make calls using the PSTN network;
- FXS Module: should be connected to an analogue phone.

In these type of cards the only configurable parameter is the LoadZone, where the country initials may be selected, so the dialtone used will be appropriate.

All ports detected as FXS will be available when editing the IVR and in the internal extensions management system. All ports detected as FXO will be available as outbound routes in the LCR management system.

3.2.8.6 Generic

This panel allows you to configure edgeBOX PBX's general options.

Logs

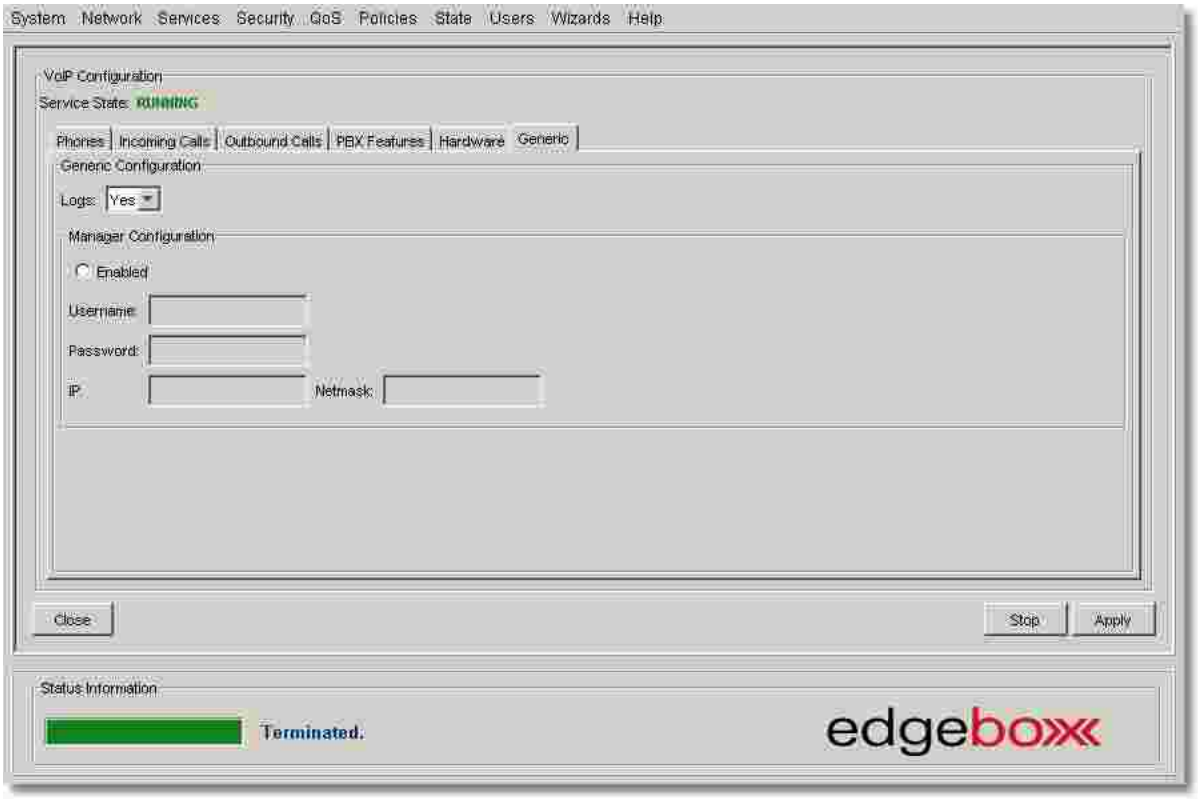
Allows you to keep logs of calls made via edgeBOX. Bear in mind that if you want to have VoIP reports you will have to set this option to "Yes", otherwise there will be no data available to display.

Manager

If you enable the manager interface you will be able to establish a telnet connection to edgeBOX's IP PBX, allowing you such diverse administration options as placing calls remotely or receiving events related to the state of calls and extensions.
This interface may be useful if you own some kind of monitoring software which you want to integrate with edgeBOX.
You will need to supply the additional information:

- Username: username used for telnet authentication;
- Password: password to be used for telnet authentication;
- IP/Netmask: IP address and netmask to me used by the remote host machine.

© 2006 Critical Links, SA



3.3 Security Menu

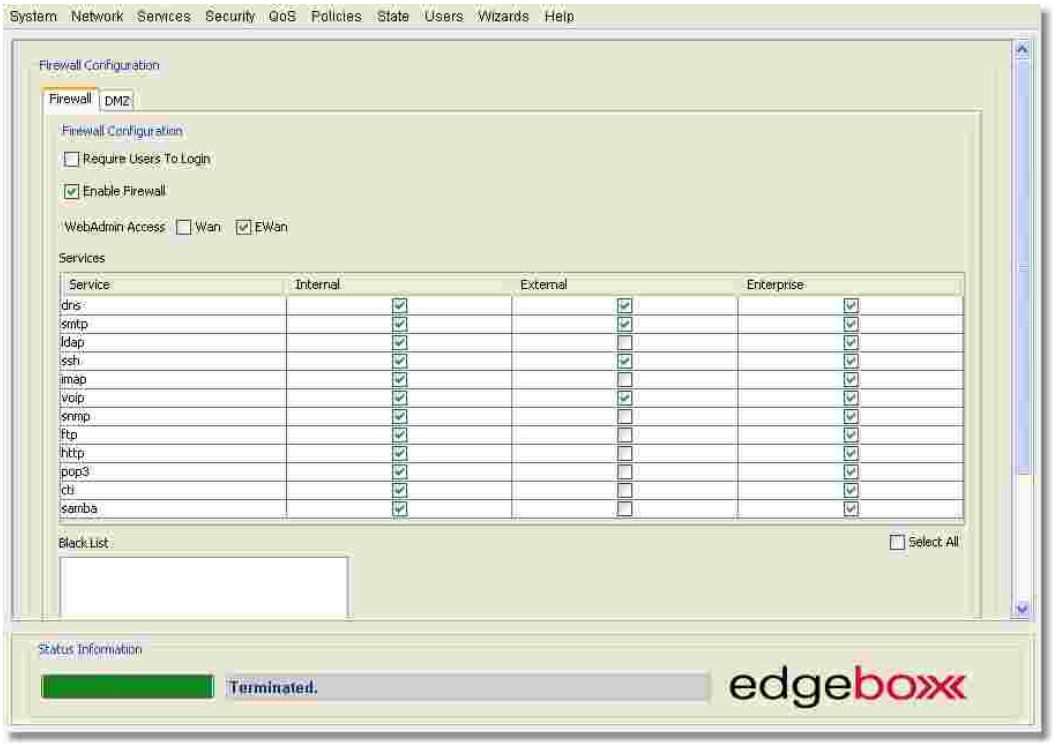
This menu option allows you to review and change security settings such as:

- Firewall (services' access, authorisation, black lists and DMZ configuration);
- NAT (enabling and port forwarding configuration);
- IPSec VPNs;
- PPTP VPNs;
- Mailscanner (engine to use, settings and actions to take) and shares' scanner.

3.3.1 Firewall

Following this menu option you will be able to review and configure your Firewall configuration. To become effective, all actions performed in this page have to be committed by pressing the Apply button on the bottom-right panel. Two panels are available: Firewall and DMZ. To access each of these panels, select the appropriate tab.

© 2006 Critical Links, SA

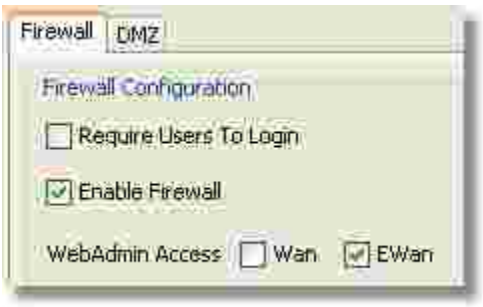


Firewall Configuration Page

3.3.1.1 Firewall

Require users to login

If you check "require users to login", users will have to authenticate (providing username/password) in order to be able to access services and resources. Granting or revoking access to services and resources is done at the group level. To know more about group policies see Policies.



Enable Firewall

If this checkbox is turned off, edgeBOX will be working in pure router mode – all services will be available. If you turn this setting on, you will be able to control access to services and filter some type of attacks. If "require users to login" is enabled then you will not be able to change this setting (it will be turned on by default).

WebAdmin Access

Wan

This checkbox controls whether the web administration interface can or cannot be accessed from the

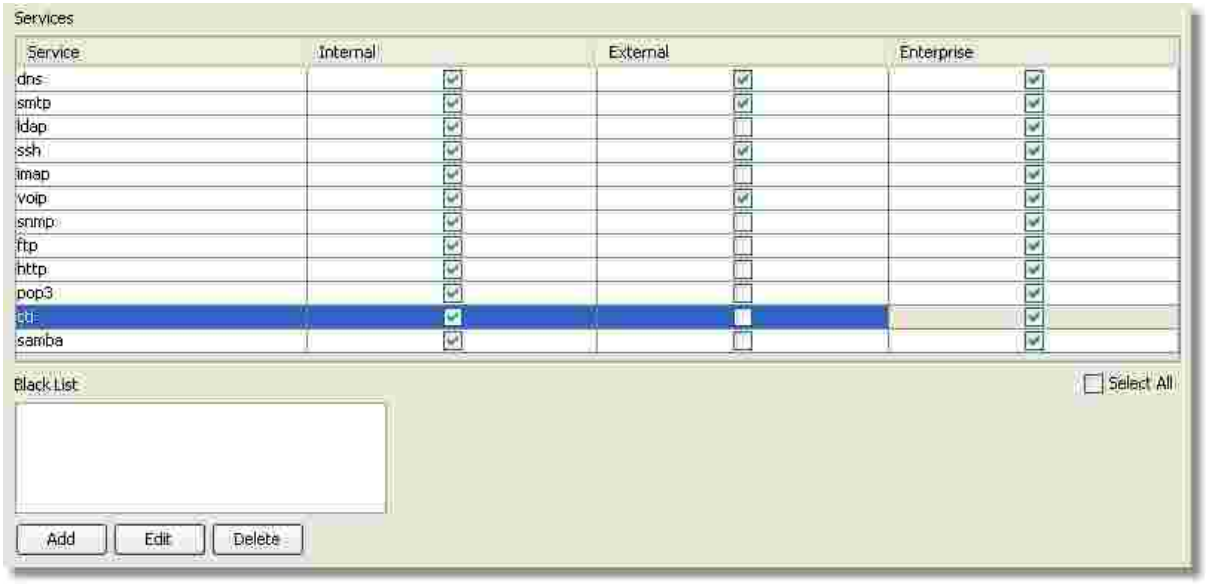
© 2006 Critical Links, SA

external network. When the firewall is enabled, this setting will be changed to “deny” automatically. Remember that if you are accessing the web interface from the external network and you deny access to it, you will not be able to reconnect again.

Ewan
This checkbox controls whether the web administration interface can or cannot be accessed from the enterprise network. Again, when you turn your firewall on, this setting will be changed to “deny”. Remember that if you are accessing the web interface from the enterprise network and you deny access to it, you will not be able to reconnect again.

Services

This panel allows you to grant or revoke access to the services running on edgeBOX for hosts in the internal, external and enterprise networks. To grant access to a service in a network, just check the cell corresponding to the intersection of the service line with the network column. When you disable the firewall, all services are enabled by default; when you enable the firewall, access to all services will be disabled.



Black List

The list applies to the external interface only. The hosts in this list will be denied any connection to edgeBOX. The actions available are Add, Edit and Delete.

Add
Selecting this option will make a pop-up window appear. Just enter the IP address for the host you want to blacklist and then press OK.

Edit
Allows you to modify an entry in the black list table. A pop-up window will appear, filled with the entry selected. Press OK to change this entry in the table.

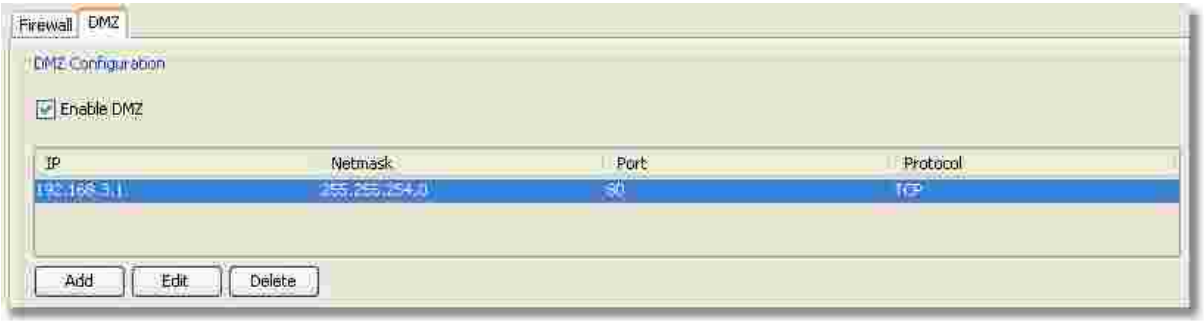
Delete
After selecting the host you want to eliminate from the list of blacklisted hosts, select “Delete”. The line will be deleted from the list. You need to select “Apply” from the changes to become effective.

© 2006 Critical Links, SA

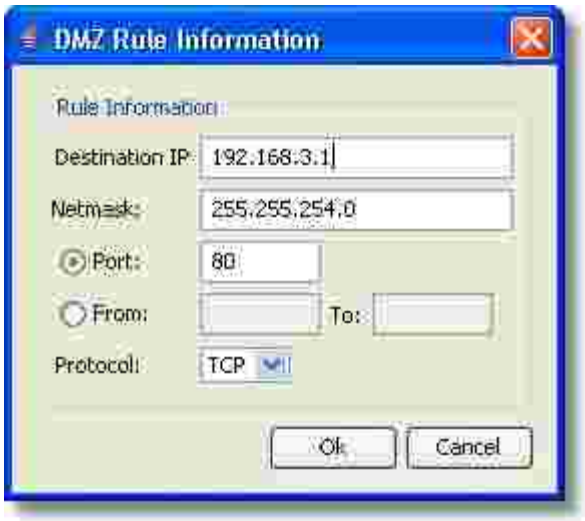
3.3.1.2 DMZ

According to the definition, a DMZ is a small subnetwork that sits between a trusted internal network (for example, a Corporate internal network) and an untrusted external network (such as the Internet). This kind of network is used as a buffer between the two networks: hosts placed in this network are accessible either from trusted and untrusted networks, but cannot access the trusted network. Usually, these kinds of networks are used to house Internet servers (web servers, DNS servers, mail servers).

The EWAN interface is used to support a DMZ in edgeBOX. This interface is configured with an IP address range accessible from the external network (in case the external network is the Internet, this range will be a public range, and so your ISP must provide routing to it). Although this address space is accessible from the external network, you will have to explicitly grant access to hosts residing in it, via appropriate rules. Next, we will show the option available for configuring a DMZ.



Enable DMZ
Checking this option will enable DMZ support. Make sure you configure an appropriate address range for the EWAN interface (EWAN Ethernet configuration panel), and that traffic with this subnetwork as its destination is being appropriately routed to edgeBOX (usually this is your ISP's responsibility). After checking this option you will need to create rules to grant access to hosts residing in this subnetwork. The rules are shown in a table which can be modified with the following options: New, Edit and Delete.



New
Allows you to enter a new rule. A pop-up window will display, requiring you to enter the following information:

© 2006 Critical Links, SA

- Destination IP: The host/range to which access will be granted;
- Netmask: The netmask to be used;
- Port: If you select this option, you will need to specify the single port to which access will be granted.
- From... To: if you select this option, you may specify a port range to which access will be granted
- Protocol: The specific protocol to which access will be granted. Choices available are TCP, UDP, ICMP and ALL.

Edit
Allows you to modify an existing rule. The options available are the same as in 'New'.

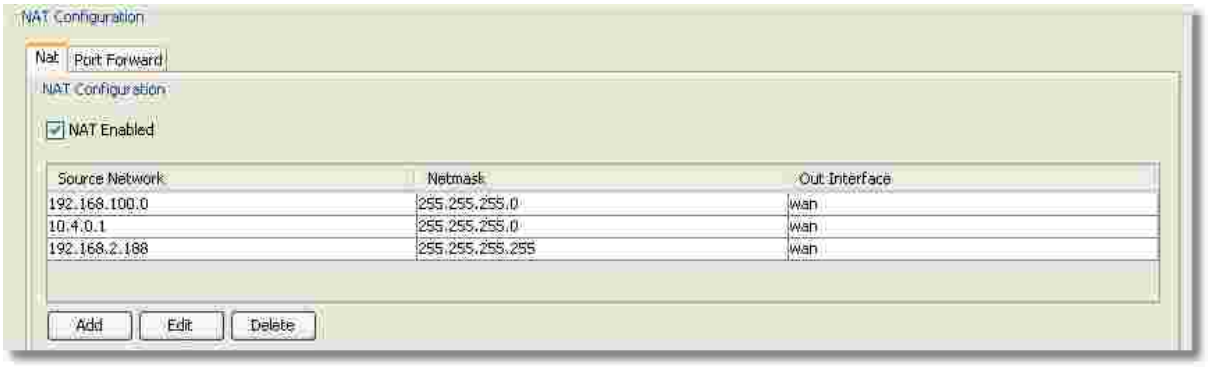
Delete
Selecting this option will eliminate the rule, revoking access to the host.

3.3.2 NAT

This page allows you to review and change the NAT configuration. With NAT you are able to use private addresses in your internal network. All requests made from internal hosts are seen by the external networks as being made by edgeBOX which then translates the response packets' destination addresses to the originating internal host.

To make changes effective, remember to select “Apply”.

Two panels are available for configuration: Nat and Port Forward, each accessible by an appropriate tab. These panels are described next.



3.3.2.1 Nat

NAT Enabled
If you want to enable NAT, check this option.

NAT Table
To configure NAT for a network the operations available are add, edit and delete.

© 2006 Critical Links, SA

Add

After selecting Add, a popup window will appear; you are required to enter the following information:

- IP: the IP address for the network to which you want to translate addresses; this is the address for the origin network (most likely, your internal network).
- Netmask: The netmask used to access hosts in this network and
- Interface: The interface used to reach this network. Select from the list, where possible values are WAN, EWAN and LAN.

Edit.

Allows you to modify an existing nat definition. The options available are the same as when entering a new NAT configuration.

Delete

To eliminate an entry for a network, just select the entry and press “Delete”. You will have to select “Apply” to make this change effective.

3.3.2.2 Port Forward

With port forwarding, you can make a service running on an internal host visible to the outside world, as if it was running on edgeBOX itself. The operations possible are “Add”, "Edit" and “Delete”. Port forwarding is available on the WAN and EWAN network interfaces.

© 2006 Critical Links, SA

Add

This option adds a new entry to the port-forwarding table. If you select add, a pop-up window will appear, requiring you to add the following information:

- External port: The port that will be seen from external networks;
- Internal IP: Internal host IP address, where the service will be running and
- Internal Port: Port where the service will be running on the internal host.

The External Range check box allows a range of ports (using the From and To fields) to mapped to the Internal IP address. Requests on all the ports in the range will be mapped to the single internal port. If the Internal Range box is checked then there is a one to one mapping from the external port number to the corresponding internal port number.

© 2006 Critical Links, SA

Edit.
Allows you to modify an existing port forwarding definition. The options available are the same as when entering a new configuration.

Delete
After selecting an entry, clickin “Delete” will eliminate that entry on the port-forwarding table.

3.3.3 VPN IPSec

In this page you can review and change your IPSec VPN configuration. These kinds of VPNs are especially suited for establishing tunnels between two private networks over the Internet, connecting them securely. Globally you can perform two actions corresponding to the buttons present in the lower panel: toggle the service status (Start/Stop) and commit your changes (Apply). The elements present in this page are described below.

© 2006 Critical Links, SA

IPSec VPN connecting two private networks

3.3.3.1 Service State

This element is read-only and gives the service status information (running or stopped).

3.3.3.2 Active Tunnels

This table shows you the active tunnels list. For each tunnel the following information will be displayed: local subnet, connection status, remote gateway and remote subnet.

3.3.3.3 VPN(s)

This table gives a list of the tunnels currently configured. Possible Operations are “Add”, “Edit” and “Delete”.

3.3.3.3.1 Add

Adds a new tunnel configuration. After selecting this option a popup window will appear where the following panels will be available:

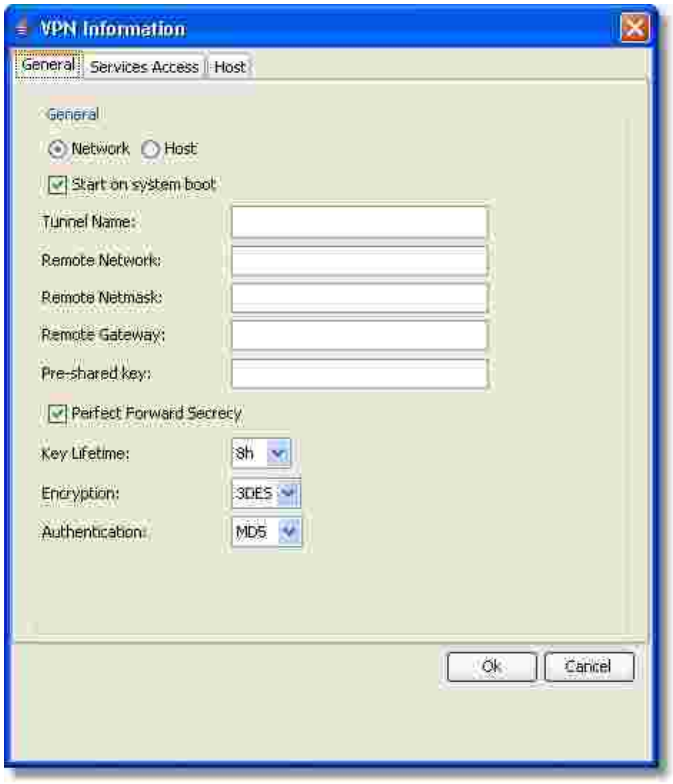
- General,
- Service Access and

© 2006 Critical Links, SA

§ Host.

3.3.3.3.1.1 General

This panel allows you to configure general VPN settings.



Choose between establishing a tunnel between the internal network and another network or between the internal network and a host. The available fields will vary according to this choice: if you've chosen “Network”, then you will have to configure a remote network, a remote netmask and a remote gateway. If you have chosen “Host”, then you will have to enter whether the host has a dynamic or static address and, in the later case, indicate which address it has.

Checking this option will activate this tunnel when edgeBOX boots.

A label chosen to identify this tunnel.

The IP address of the network we want to establish a tunnel with.

Netmask to apply to the remote network IP address.

The IP address for the gateway connecting to the remote network. This will be a public address.

© 2006 Critical Links, SA

Checking this option will allow you to enter the remote host IP.

This option will be available only if the previous checkbox is on. This will be the address of the host to which the tunnel will be established.

Checking this option will activate automatic keying. In this mode keys are automatically generated on connection establishment and periodically generated thereafter.

The expiration time for a shot-term key (the time after which a new key will be generated).

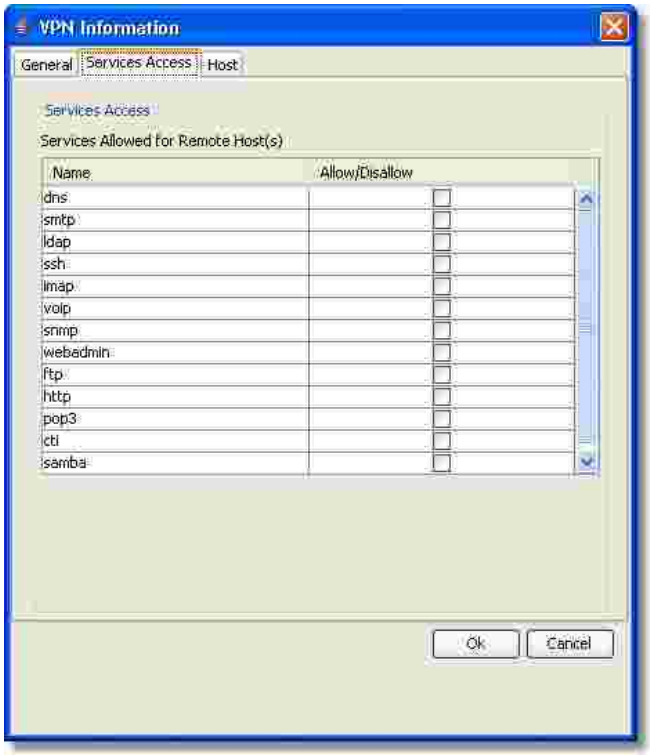
Algorithm used for encryption. Available choices are 3DES and AES.

Algorithm used for authentication. Available choices are MD5, SHA1 and SHA2.

3.3.3.3.1.2 Services Access

Services Allowed for Remote Host(s)

In this table you can grant or revoke access to services running on edgeBOX for hosts in the external network. Check the cell corresponding to service desired to grant access, uncheck it to revoke access.



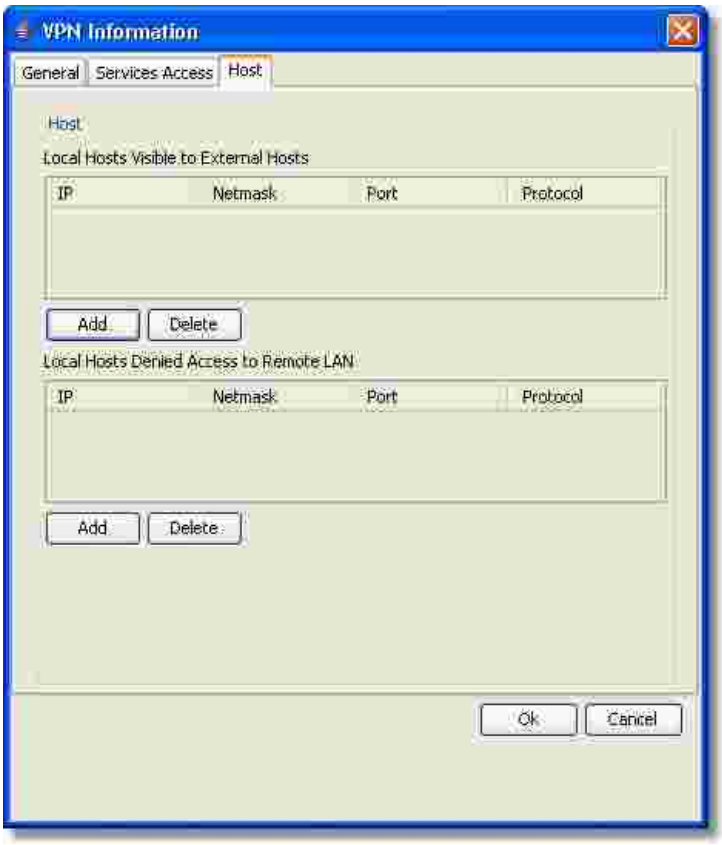
3.3.3.3.1.3 Host

This panel allows you to configure access lists, specifically:

© 2006 Critical Links, SA

§ To allow access to your network hosts from hosts in the remote network and

§ To deny some of your local hosts access to the remote network.



By default, external hosts will not have access to any host in the network. This option allows you to configure local hosts' visibility from the external network. Available actions are “Add” and “Delete”.

Add

After selecting “Add”, a popup window will appear, requesting the following information:

- Origin: The IP address for the host in the network to which we want to grant access;
- Netmask: The netmask to apply;
- Port: The port which we want to grant access. This option may be disabled or ignored, depending on your choice of protocol;

A range of ports may be specified by checking the Range box. The ports listed in the From and To fields will be granted access.

- Protocol: Select from the list. Available choices are: TCP, UDP, ICMP and ALL. If ALL or ICMP are selected then “Port” will be ignored.

Delete

Deletes an entry from this table. After selecting the entry, press “Delete”. Removing an entry from this table is the same as denying access to the host/service from hosts in the external network.

© 2006 Critical Links, SA

By default all hosts in the network will be able to use the tunnel. This option allows you to configure local hosts' access to the tunnel. Available actions are “Add” and “Delete”.

Add
After selecting “Add”, a popup window will appear requesting the following information:

- Origin: The IP address for the host in the network to which we want to deny access to the tunnel;
- Netmask: The netmask to apply;
- Port: The port which we want to deny access to. This option may be disabled or ignored, depending on your choice of protocol;

A range of ports may be specified by checking the Range box. The ports listed in the From and To fields will be denied access.

- Protocol: Select from the list. Available choices are: TCP, UDP, ICMP and ALL. If ALL or ICMP are selected then “Port” will be ignored.

Delete
Deletes an entry from this table. After selecting the entry, press “Delete”. Eliminating an entry from this table is the same as granting access to the tunnel for a host in the network.

3.3.3.3.2 Edit

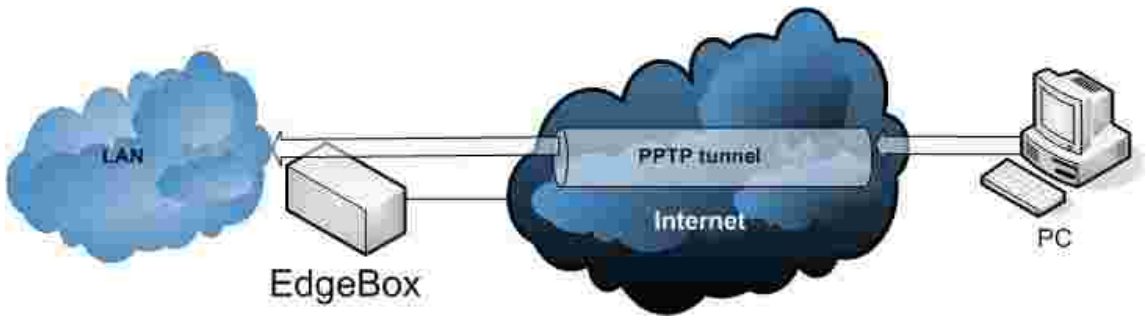
This option allows you to change an IPSec tunnel configuration. Select a tunnel from the list and a popup window similar to the one in “Add” will appear. You can change the same options.

3.3.3.3.3 Delete

Removes a tunnel configuration. Select the IPSec tunnel you want to delete and then select the “Delete” button.

3.3.4 VPN PPTP

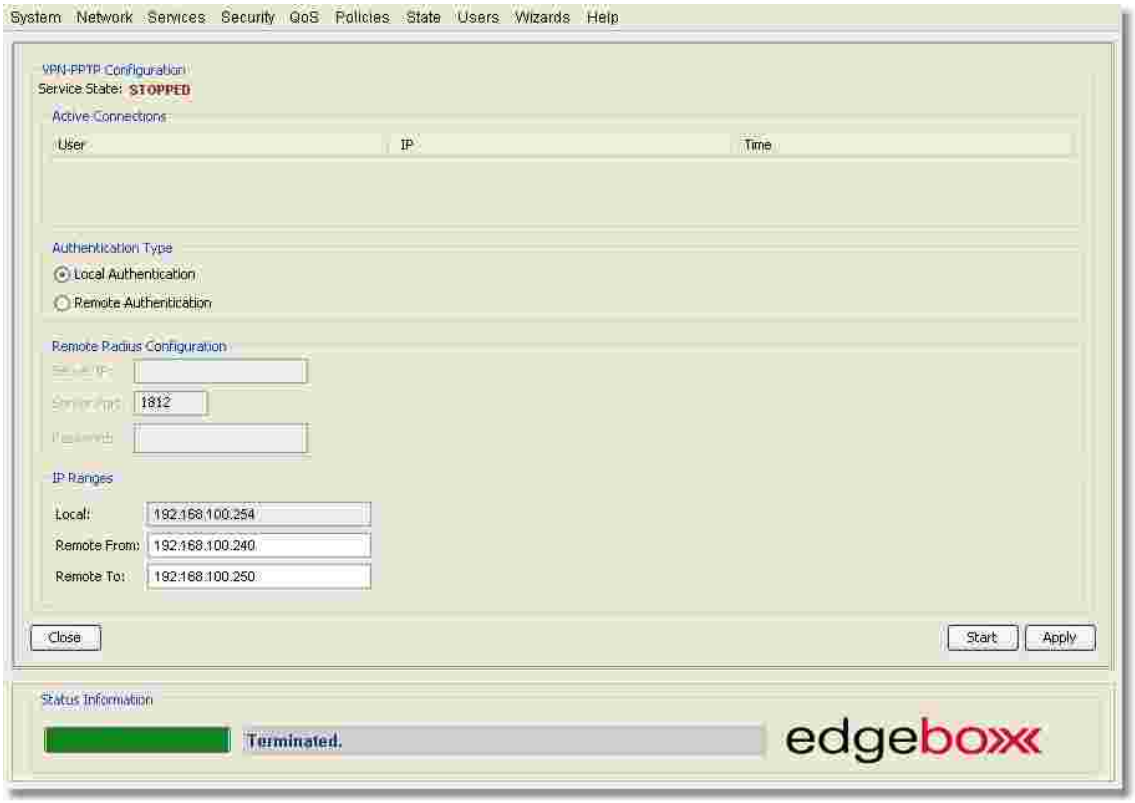
In this page, you can review and change your PPTP VPN configuration. PPTP is used to establish VPN tunnels across the Internet. This allows remote users to access the internal network from anywhere on the Internet. On this page you have two operations available: starting/stopping the service or applying changes made to the configuration. You will trigger these actions selecting the buttons on the lower panel.



PPTP tunnel connecting a host to a private network

© 2006 Critical Links, SA

The available elements in this page are described next.



3.3.4.1 Service State

This information is read-only and gives you the current status of the service. Possible values are running and stopped.

3.3.4.2 Connected users

A table where each connected user is listed as well as the IP address of the client machine from where the connection was established, and the time at which the connection was established.

3.3.4.3 Authentication Type

Authentication can be performed either by the Radius server running on the edgeBOX or by an external Radius server.

3.3.4.3.1 Local Authentication

Selecting "Local Authentication" means that the authentication will be performed by edgeBOX's Radius server. No additional configuration is needed, such as Radius user creation. Authorisation for PPTP VPN use is configured in the User Management panel.

© 2006 Critical Links, SA

3.3.4.3.2 Remote Authentication

Displays the remote Radius server used to authenticate users.

Add
Selecting “Add” makes a popup window will appear requesting you the following information:

- Server IP: IP address for the Radius server;
- Server Port: The port where the radius daemon is running;
- Password: shared secret between edgeBOX and the radius server;
- Timeout: amount of time after which the connection will timeout (in seconds).

After selecting “OK”, you have to select “Apply” in the main panel to make changes effective.

Delete
After selecting an entry, select “Delete” to eliminate it from the table. You have to select “Apply” to make this change effective.

3.3.4.4 IP ranges.

This element has the following information:

Local
This is edgeBOX's LAN interface IP address. The remote client PC will use this address as the

© 2006 Critical Links, SA

gateway for the private network. This information is read-only.

Remote From and Remote to
These two fields allow you to set the IP address range which will be assigned to clients connecting through PPTP.

3.3.5 MailScanner

In this page you can review and change edgeBOX's MailScanner options. New in edgeBOX version 4 is the ability to scan edgeBOX's windows shares and support for the McAfee virus scanning engine.

MailScanner Page

Currently, support is available for three antivirus engines, Sophos, McAfee and ClamAV. edgeBOX is not shipped with the Sophos or the McAfee antivirus engines installed, so you will have to buy the appropriate number of licenses to use and upload them to edgeBOX.

The following panels are available for configuration, each accessible through a named tab:

- Shares Scanner,
- Mail Scanner and
- Anti-Virus Engines.

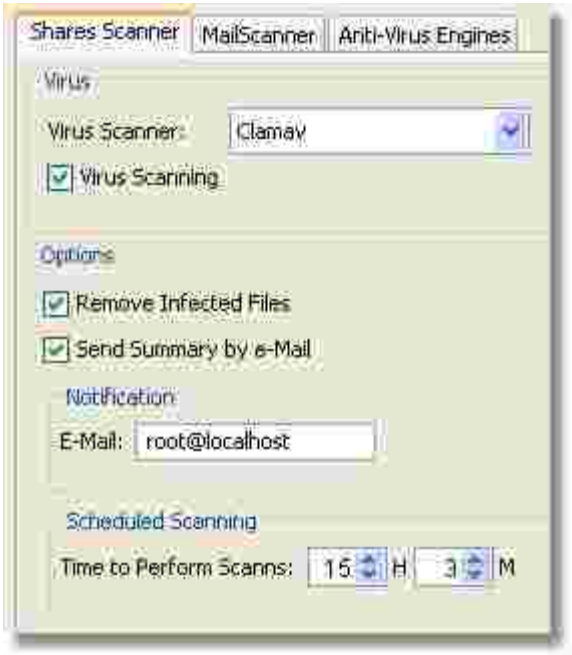
We will describe each of these panels in the following sections.

© 2006 Critical Links, SA

3.3.5.1 Shares Scanner

This panel allows you to configure edgeBOX's shares scanner. Options include:

- Enabling shares scanning and choosing the engine to use;
- General options such as scheduling, notifications and infected file deletion.



3.3.5.1.1 Virus

Virus Scanner
The Virus Scanning package to use. Possible choices are Sophos, McAfee, ClamAV or None.

Virus Scanning
Check this option if you want to enable virus scanning.

3.3.5.1.2 Options

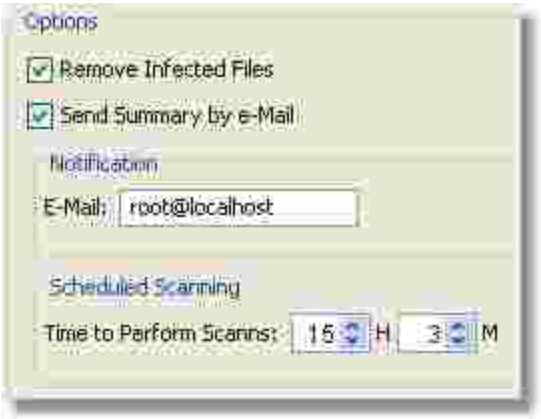
Remove Infected Files
If you check this option, then files found to be infected will be deleted.

Send summary by e-Mail
Check this option if you want a shares' scan report to be sent by email.

© 2006 Critical Links, SA

Notification E-mail
The email address where the shares' scan report will be sent.

Scheduled Scanning
Use this option to configure the time when scans will be performed.



3.3.5.2 Mail Scanner

Allows you to configure the Mailscanner settings. The following panels are available for configuration, accessible through the named tabs located on the right:

- General,
- Messages and
- Actions.

3.3.5.2.1 General

Allows you to configure general Mailscanner configurations. Available options are:

- Antivirus engine selection,
- Spam options and
- Notification options.

© 2006 Critical Links, SA

3.3.5.2.1.1 Virus

Virus Scanner

The Virus Scanning package to use. Possible choices are Sophos, McAfee, ClamAV and None.

Virus Scanning

Check this option if you want to enable virus scanning.

© 2006 Critical Links, SA

3.3.5.2.1.2 Spam

Spam Checks
Check this option if you want the MailScanner to check if incoming messages are spam.

Log Spam
Check this option if you want the MailScanner to log spam messages to syslog.

Spam Actions
The action to be applied to spam messages. Choose from the list of allowed values, which may be:

- Deliver: The message is delivered to the recipient as normal;
- Delete: The message is silently discarded;
- Bounce: A rejection message is sent to the sender and
- Attachment: The original message is converted to the attachment of the message.

RBL Servers
This feature allows you to have a anti-spam protection based on existing spammers' databases (The Realtime Blackhole List). After checking this option you will have to provide hosts serving these lists. To manage the list you have two options: “Add” and “Delete”.

Add
Inserts a new host in the list of hosts that will be queried to check if the incoming mail domain was blacklisted. After selecting 'Add', a popup window will appear. Insert the hostname and select “OK”.

© 2006 Critical Links, SA

You then have to select “Apply” for changes to become effective. You can have as many hosts as you like. At the time of this publication examples of hosts providing such lists are: list.dsbl.org, sbl.spamhaus.org and bl.spamcop.net.

Delete
Deletes an entry for a host from the list. You have to select “Apply” to make this change effective.

3.3.5.2.1.3 More Options

Notify Sender
If you check this option, notifications will be sent to infected messages’ senders.

Send Notices
If you check this option, then every time a spam message is received a specific user will be notified.

Notices To
This field will only be enabled if you check the previous option. This is the user who will receive the notifications every time a spam message is received.

© 2006 Critical Links, SA

3.3.5.2.2 Messages

Allow Partial Messages

If you check this option you will allow messages that contain only a fraction of the attachments. As the scan is not performed on the whole message but on its fragments, it will not be done properly. Setting this option is very dangerous as viruses may go undetected.

Allow External Message Bodies

If you check this option you will allow messages where the body is stored in a remote server and not in the actual message. It will be up to the email client to fetch the message body later. Again, setting this option is particularly dangerous because MailScanner never scans the message body so it may allow viruses into your network.

Allow Iframe Tags

If you check this option you will allow your messages to carry Iframe tags.

Log Iframe Tags

If you check this option you will enable logging of messages with Iframe tags.

Allow Form Tags

If you check this option you will allow your messages to carry Form tags.

Allow Object Codebase Tags

If you check this option you will allow your messages to carry Object codebase tags.

Convert Dangerous HTML to Text

If you check this option you will enable the conversion of Iframe and Object codebase tags into plain

© 2006 Critical Links, SA

text. This is a good alternative to disallowing or leaving them untouched.

Convert HTML to Text
If you check this option you will enable the conversion of all HTML tags into plain text.

Block Encrypted Messages
If you check this option you will enable blocking of encrypted messages.

Block Unencrypted Messages
If you check this option you will enable blocking of unencrypted messages.

Expand TNEF
If you check this option you will enable expanding of TNEF attachments that are joined in one WINMAIL.DAT file. If you don't check this option then the filenames within the TNEF attachments will not be checked.

3.3.5.2.3 Actions

Deliver Disinfected Messages
If you check this option then infected attached documents will be automatically disinfected and sent to the original recipients.

Quarantine Infections
If you check this option then infected/dangerous attachments will be stored in directories created under the quarantine directory.

Quantantine Whole Message

© 2006 Critical Links, SA

If you check this option then the whole message will be stored in quarantine and not just the attachments.

Deliver Unparsable TNEF
If you check this option you will allow the delivery of Rich Text Format attachments produced by some versions of Microsoft Outlook that cannot be completely decoded at present.

Still Deliver Silent Viruses
If you check this option messages that originally contained a silent virus will still be delivered, even if the addresses were chosen at random by the infected PC and did not correspond to anything a user intended to send.

Sign Clean Messages
If you check this option MailScanner will sign every clean message processed.

Mark Infected Messages
If you check this option MailScanner will mark every infected message and every message that, for some reason had its attachments removed.

Mark Unscanned Messages
If you check this option every message not scanned by MailScanner will be marked.

Warning Is Attachment
If you check this option then warnings for dangerous or infected attachments will be included as an attachment. If this option is not selected then the warnings will simply be included as inline text.

3.3.5.3 Anti-Virus Engines

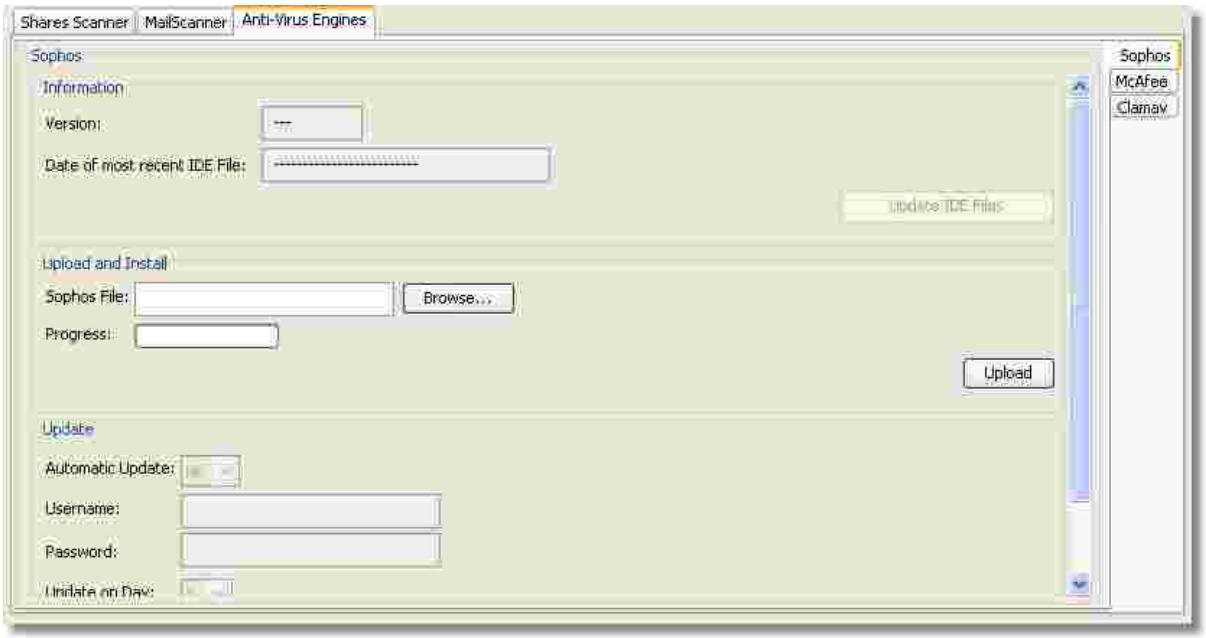
This panel allows you to perform the installation of anti-viruses' engines (where applicable), and update their IDE files. Select the desired antivirus engine using the named tab on the right. Currently the supported anti-viruses engines are:

- Sophos,
- McAfee and
- Clamav.

© 2006 Critical Links, SA

3.3.5.3.1 Sophos

This panel allows you to upload the Sophos antivirus engine required to perform antivirus scans. Remember that you will have to buy an appropriate number of licenses in order to use this engine. You may also check the virus definitions database version and update it.



Sophos Options

© 2006 Critical Links, SA

3.3.5.3.1.1 Information

This panel contains the elements described next.

Version
The antivirus engine version installed. This element is read-only.

Date of most recent IDE files
The date of the last virus definitions file installed.

Update IDE Files
Selecting this button will download the latest virus definition files. You must have a current license for Sophos in order to do this. The edgeBOX also performs this update automatically on a daily basis.

3.3.5.3.1.2 Upload and Install

This panel allows you to install a Sophos antivirus engine:

- Download the antivirus engine from the Sophos website. Bear in mind that you need to buy the appropriate number of licenses to use this software;
- Hit the “Browse” button and navigate to the location where you saved the antivirus engine file. Select it.
- Hit the “Upload” button and wait until the progress bar reaches 100%. Check the status returned to confirm the command was successful. This transfer is done via FTP so make sure that FTP traffic is allowed on the LAN side on your firewall configuration.

3.3.5.3.1.3 Update

This panel allows the edgeBOX to keep the Sophos antivirus engine automatically updated on a monthly basis. Please enter the username and password you received with your Sophos License registration and select the day of the month for this update to be executed.

© 2006 Critical Links, SA

3.3.5.3.2 McAfee

This panel allows you to upload the McAfee antivirus engine required to perform antivirus scans. Remember that you will have to buy an appropriate number of licenses in order to use this engine. You may also check the virus definitions database version and update it.

3.3.5.3.2.1 Information

This panel contains the following elements:

Version
The antivirus engine version installed. This element is read-only.

Date of most recent IDE files
The date the last virus definitions file was installed.

Update IDE Files
Selecting this button will download the latest virus definition files.You must have a current Sophos license in order to do this. The edgeBOX also performs this update automatically on a daily basis.

3.3.5.3.2.2 Upload and Install

This panel allows you to install a McAfee antivirus engine:

- Download the antivirus engine from the McAfee website. Bear in mind that you need to buy the appropriate number of licenses to use this software.
- Hit the “Browse” button and navigate to the location where you saved the antivirus engine file. Select it.

© 2006 Critical Links, SA

- Hit the “Upload” button and wait until the progress bar reaches 100%. Check the status returned to confirm the command was successful. The transfer is done via FTP so make sure that FTP traffic is allowed on the LAN side on your firewall configuration.

3.3.5.3.3 Clamav

This panel allows you to check and update Clamav's IDE files. Clamav is a free antivirus engine and is shipped with edgeBOX.

Version
The antivirus engine version installed. This element is read-only.

Date of most recent IDE files
The date of the last virus definitions file installed.

Update IDE Files
Selecting this button will download the latest virus definition files. edgeBOX also performs this update automatically on a daily basis.

© 2006 Critical Links, SA

4 Advanced Topics

In this chapter, we will cover advanced configuration options such as:

- User and group management;
- Group policies;
- Quality of service for groups and services;
- System configuration;
- State information and
- The CLI.

4.1 User and Group Management

User and group management are some of the key functions of edgeBOX. If you have user authentication turned on, access to services and resources will be granted only if the user provides their credentials (username and password). Users will exist in the context of a group and, as we will see in Policies, there are several items which can be configured to form a policy to apply to a group. A policy thus defines the type of access users in a group have to items such as the Internet, services running on the box, the enterprise network and VPNs.

Additionally, there is the ability to specify which services a user will be able to use. This is done during user creation.

In this section we will see how to deal with user and group management.

To access user and group management, choose the Users menu option and then the Management submenu. A page like the one shown bellow will be displayed. On this page you have two panels: the Users and the Groups panel. You may access each panel selecting the appropriate tab.

© 2006 Critical Links, SA

User Management Page

4.1.1 Users

You can check the users listed in the table. Available actions for users are “New”, “Edit” and “Delete”.

© 2006 Critical Links, SA

New User Window

New

Creates a new user. After selecting “New”, a popup window similar to the one shown above will be displayed, requiring you to enter the following information:

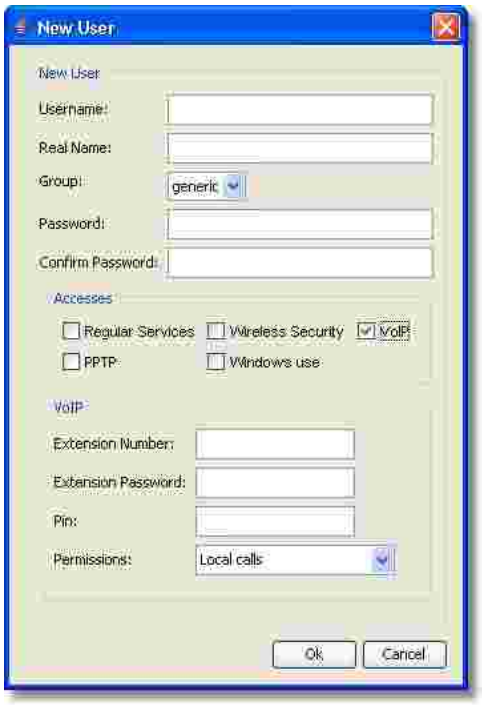
- Username: The login name that will identify this user on edgeBOX. The login name cannot be greater than 8 characters, has to start with a non-numeric character and cannot contain special characters.
- Real Name: This field is optional and is meant to identify the user. No special characters can be used.
- Group: The group to which this user will be assigned. If no groups are available at the time of creation, a group named ”generic” will be created and this user will be added to it.
- Password and Confirm Password: The password to be used by this user to authenticate on the system. The user is advised to choose the password carefully, following a set of well-known guidelines (not using any infomration personally related to them, mixing characters with non-alphanumeric symbols, etc…).
- Accesses: The services this user will be able to use. Check the services desired to enable access to them. Available options are regular services (services running on edgeBOX such as SMTP, POP3, FTP and the Internet), Wireless (if 802.1x authentication is used), VoIP, PPTP and Windows use (Samba).

If you check VoIP then additional options will be available for configuration:

- § Extension Number: The extension number to be used by this user.
- § Extension Password: The password used to register.
- § Pin: The pin to be entered if authentication is turned on, to check which type of calls the user has permission to make.
- § Permissions: The type of calls the user is allowed to make. Available options are Local calls, Long distance calls, Mobile calls, International calls and Any type of calls. Each of these types include its predecessors, so Long distance calls include Local

© 2006 Critical Links, SA

calls, Mobile calls include both Long distance calls and Local calls, and so on.



Edit

After selecting the user you want to change from the users table and selecting “Edit”, a popup window will appear. This popup will be similar to the one displayed when a “New” record was added, except that you will not be able to change the username. A table will also appear, displaying the users' quota settings and you will not be able to change extension details in voip settings.

After changing the desired fields, selecting “OK” will make them effective and “Cancel” will abort them. If you want to keep the users' password unchanged, leave the fields blank; otherwise the password will be updated.

Delete

Deletes a user from the system. After selecting the user from the users' table, selecting “Delete” will immediately remove the user.

If you have authentication set to remote, a remote server will validate credentials entered by a user. A user and directory structure will be created locally when the first successful login occurs. Unless the user was previously created and assigned to a group, they will be placed in the 'generic' group. You must always create groups and users, and assign them before the users login to the system.

© 2006 Critical Links, SA

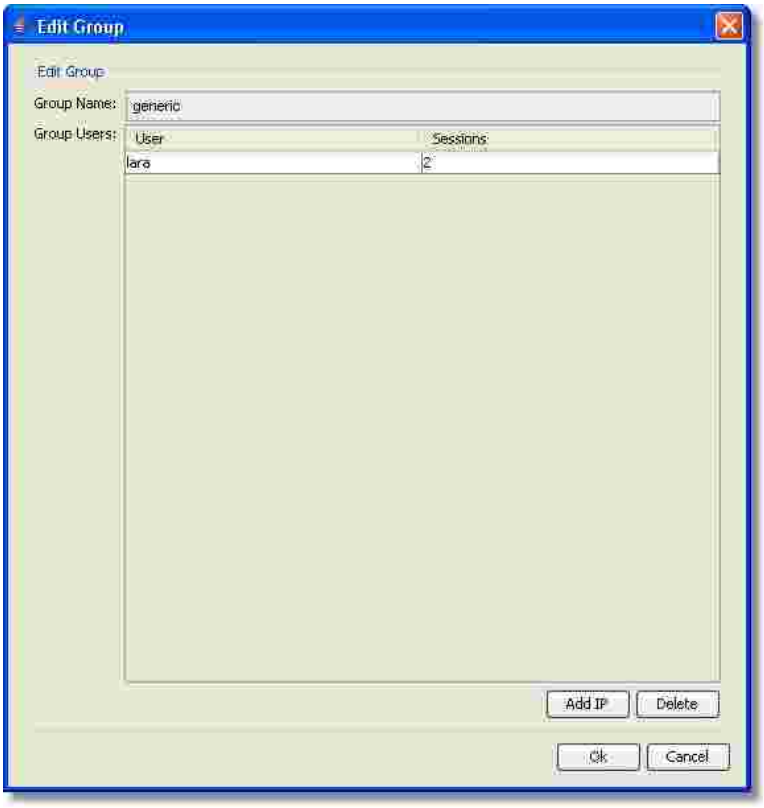
4.1.2 Groups

Regardless of the authentication scheme chosen (Local or Remote), you should check if a group called “generic” already exists. This is the group where users will be placed by default, so you must ensure that it exists and configure its policies before users log into your network.

The options available are: “New”, “Edit” and “Delete”.

New
Creates a new group. After selecting “New” a window will popup requiring you to enter the new group name. After selecting “OK” the new group will be immediately created. Selecting “Cancel” will abort the group creation.

© 2006 Critical Links, SA



Edit Group Window

Edit

After selecting the group from the list, “Edit” will make a popup window similar to the one shown above appear. In this window are listed the users and IP for the group selected. Available options are “Add IP” and “Delete”.

Add IP

Besides containing users, a group may also contain IP addresses. In Policies you will see why you may be interested in having machines as members of a group. After selecting “Add IP” a popup window will appear asking you to enter the IP address. After selecting “OK”, you still have to select “OK” in the main popup for the changes to become effective.

Delete

After selecting the user or IP address you want to remove, select “Delete”. You will have to select “OK” in the main popup for changes to become effective. If you have selected a user, they will be assigned to the generic group; if you have selected an IP address, it will be removed.

Delete

After selecting a group, “Delete” will remove it. All users belonging to this group will be assigned to the group “generic”. All IPs assigned to this group will be deleted.

4.2 Policies

Policy group configuration will be covered in this section. We will see the items available for configuration that, as a whole, will form a policy to apply to a group. To access group policies choose, in the menu “Policies”, the submenu “Groups”. A page similar to this will be displayed:

© 2006 Critical Links, SA

Policy Groups Configuration

On this page is a list of groups and their access to the services running on the box, to the Internet and to the enterprise network. If the cell is unchecked then the group has no access to this resource; if the cell is checked then the group has some level of access to this resource.

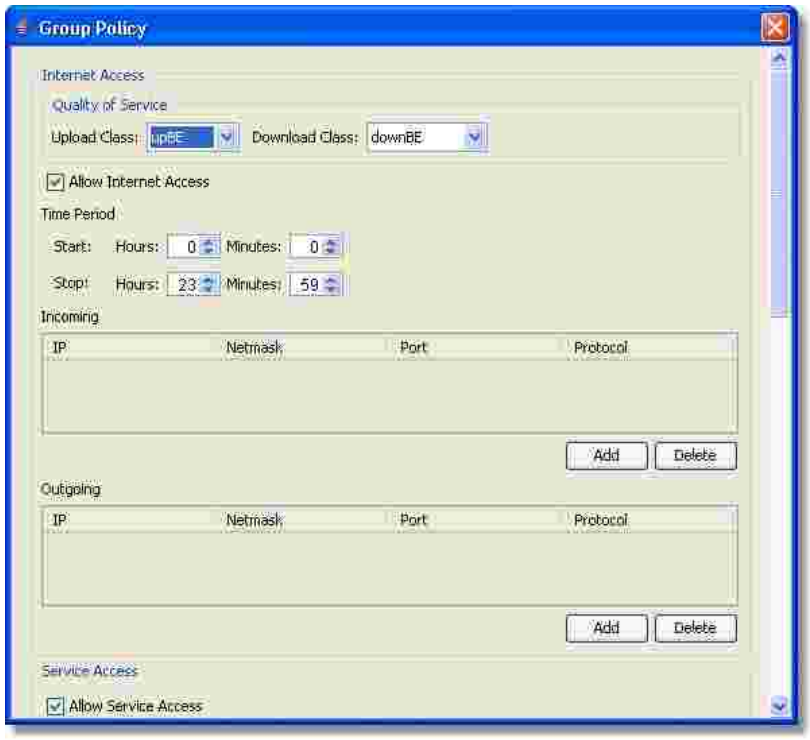
4.2.1 Editing a Group Policy

To edit a policy for a group select the row corresponding to the desired group and select “Edit”. The following options can be configured:

- Internet Access;
- Service Access;
- Enterprise Access;
- VPN Connections;

© 2006 Critical Links, SA

4.2.1.1 Internet Access



Group Policy Edit Window

This panel allows configuration of the Internet access options. The available items are:

- Quality of Service and
- Allow Internet Access.

4.2.1.1.1 Quality of Service

You can set both an upload class and a download class (for more details on quality of service, check Traffic Control). The default values are upBE and downBE, meaning all traffic will have the same treatment. You can, however, choose from the lists to give the Internet traffic to and/or from this group some priority by selecting another value.

4.2.1.1.2 Allow Internet Access

If this option is unchecked this group will not have access to the Internet, so the next panel will be disabled. If you check this option you may then fine-tune Internet access using the options available in the next panel, which are the following:

- Time Period,
- Incoming and
- Outgoing.

© 2006 Critical Links, SA

4.2.1.1.2.1 Time Period

You can grant access for the whole day (the default) or just to a time interval. Insert the limits for this interval directly in the fields or using the up-down controls.

4.2.1.1.2.2 Incoming

By default all incoming traffic from the Internet is denied access to the internal network. With this option you can allow incoming traffic based on its origin, port and/or protocol. This table displays the list of allowed connections. The options available are “Add” and “Delete”.

Add

Creates a new entry in the table. After selecting “Add”, a popup window similar to the one shown will appear requiring you to enter the following information:

Add Allowed Incoming Connection Window

- Origin IP: The IP address for the host/network which is starting the connection we want to allow;
- Netmask: The netmask to apply;
- Port: The service port we want to allow access to; this option will be disabled if the protocol chosen is either “ICMP” or “ALL”;

The Range check box allows a range of ports (using the From and To fields) to be specified for the incoming traffic.

- Protocol: Select from the list. Possible values are: TCP, UDP, ICMP and ALL.

After selecting “OK” you will also have to select “OK” in the main panel for changes to become effective.

Delete

Deletes an entry from the table, denying traffic for this connection. After selecting the entry from the table, selecting “Delete” will remove it. You have to select “OK” in the main panel for changes to become effective.

© 2006 Critical Links, SA

Allowing incoming connections will only apply if NAT is not active for the external interface, i.e. the edgeBOX is working in pure router mode for this interface. If this is not the case, the internal network will not be visible from the outside and connections will always have to originate from the inside.

4.2.1.1.2.3 Outgoing

By default, all outgoing traffic is allowed, i.e. traffic originating from the internal network to the Internet is granted access. With this option we can deny outgoing traffic based on its destination, port and/or protocol. This table displays the list of connections denied. The options available are “Add” and “Delete”.

Add
Creates a new entry in this table. After selecting “Add” a popup window will appear requiring you to enter the following information:

- Destination IP: Host or network address which we want to deny connections to;
- Netmask: The netmask to apply;
- Destination Port: The service port we want to deny access to. This option will be disabled if the protocol chosen is either “ICMP” or “ALL”.

The Range check box allows a range of ports (using the From and To fields) to be specified for the outgoing traffic.

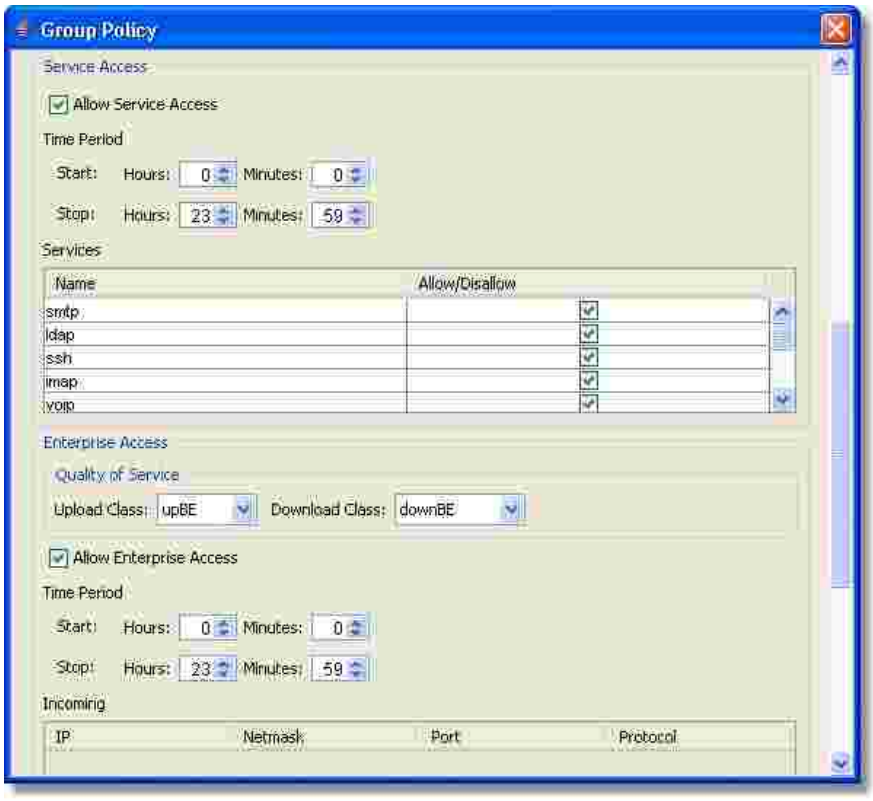
- Protocol: Select from the list. Possible values are: TCP, UDP, ICMP and ALL.

After selecting “OK” you will also have to select “OK” in the main panel for changes to become effective.

Delete
Deletes an entry from the table, allowing traffic for this connection. After selecting the entry from the table, selecting “Delete” will remove it. You have to select “OK” in the main panel for changes to become effective.

© 2006 Critical Links, SA

4.2.1.2 Service Access



Service Acesss

In this panel we can configure the access options for the services. The items available for this option are:

Allow Service Access
If this option is unchecked the group will not have access to the services running on the box and the next panel will be disabled. If you check this option you may then fine-tune service access using the options available in the next panel, which are described below.

Time Period
You can grant access for the whole day (the default) or just to a time interval. Insert the limits for this interval directly in the fields or using the up-down controls.

Services
In this table you can choose exactly what services the group will be able to access. A check in the cell's service will grant access; not checking it will revoke access to it.

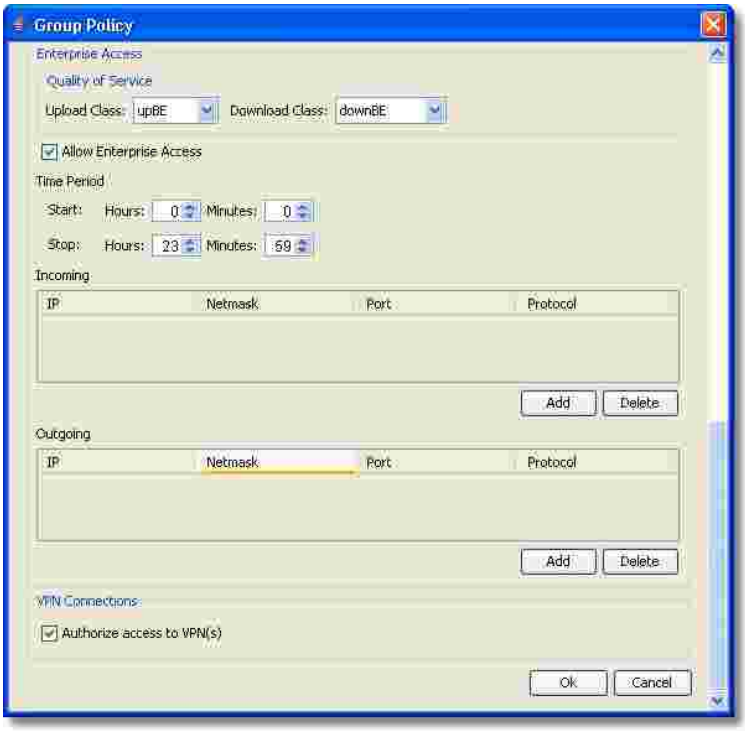
4.2.1.3 Enterprise Access

In this panel, we can configure the enterprise access options. This panel works in a similar way to the Internet access panel, except that this one applies to the enterprise network. The available items are:

- Quality of Service and

© 2006 Critical Links, SA

- Allow enterprise access.



4.2.1.3.1 Quality of Service

You can set both an upload class and a download class (for more details on quality of service, see Traffic Control). The default values are upBE and downBE, meaning all traffic will have the same treatment. You can, however, choose from the lists to give the Internet traffic to and/or from this group some priority by selecting another value.

4.2.1.3.2 Allow enterprise access

If this option is unchecked, this group will not have access to the enterprise network and the next panel will be disabled. If you check this option, you can then fine-tune enterprise access using the options available in the next panel, which are:

- Time Period,
- Incoming and
- Outgoing.

4.2.1.3.2.1 Time Period

You can grant access for the whole day (the default) or just to a time interval. Insert the limits for this interval directly in the fields, or using the up-down controls.

© 2006 Critical Links, SA

4.2.1.3.2.2 Incoming

By default, all incoming traffic from the enterprise network is denied access to the internal network. With this option, you can allow incoming traffic based on its origin, port and/or protocol. This table displays the list of allowed connections. The options available are “Add” and “Delete”.

Add
Creates a new entry in the table. After selecting “Add”, a popup window will appear requiring you to enter the following information:

- Origin IP: The IP address for the host/network we want to allow which is starting the connection;
- Netmask: The netmask to apply;
- Port: The service port we want to allow access to; this option will be disabled if the protocol chosen is either “ICMP” or “ALL”;

The Range check box allows a range of ports (using the From and To fields) to be specified for the incoming traffic on the EWAN network interface.

- Protocol: Select from the list. Possible values are: TCP, UDP, ICMP and ALL.

Delete
Deletes an entry from the table, denying traffic for this connection. After selecting the entry from the table, selecting “Delete” will remove it. You have to select “OK” in the main panel for changes to become effective.

Allowing incoming connections will only apply if NAT is not active for the enterprise interface, i.e. the edgeBOX is working in pure router mode for this interface. If this is not the case, the internal network will not be visible from the enterprise and connections will always have to originate from the inside.

4.2.1.3.2.3 Outgoing

By default, all outgoing traffic is allowed, i.e. traffic originating from the internal network to the enterprise network is granted access. With this option, outgoing traffic can be denied based on its destination, port and/or protocol. This table displays the list of connections denied. The options available are “Add” and “Delete”.

Add
Creates a new entry in the table. After selecting “Add”, a popup window will appear requiring you to enter the following information:

- Destination IP: Host or network address which we want to deny connections to;
- Netmask: The netmask to apply;
- Destination Port: The service port we want to deny access to. This option will be disabled if the protocol is either “ICMP” or “ALL”.

The Range check box allows a range of ports (using the From and To fields) to be specified for the outgoing traffic on the EWAN network interface.

- Protocol: Select from the list. Possible values are: TCP, UDP, ICMP and ALL

Delete
Deletes an entry from the table, allowing traffic for this connection. After selecting the entry from the table, selecting “Delete” will remove it. You have to select “OK” in the main panel for changes to become effective.

© 2006 Critical Links, SA

4.2.1.4 VPN Connections

If “Authorise access to VPN(s)” is checked, then we are allowing the members of the group to use IPSEC VPN tunnels; otherwise access is denied. Bear in mind that this definition will override the access granted in the VPN configuration.

4.3 Traffic Control

Traffic Control Configuration Page

As we've seen, one of the elements you can configure in a policy is the traffic control class. With this setting, you may assign a special priority to the traffic coming from or going to a given group, resulting in a better service for the group. Before this setting becomes effective you have to configure and start the traffic control service. To access the configuration page, select the QoS menu option and then the Traffic Control submenu option. A page like the one shown above will display. Possible actions are: Start/Stop, depending on whether the service is stopped or running, and Apply, which will be used when you want to change an existing configuration. The available options are similar for each interface, so we will just cover the WAN interface. The available options are:

- Service State,
- Upload Information and
- Download Information.

4.3.1 Service State

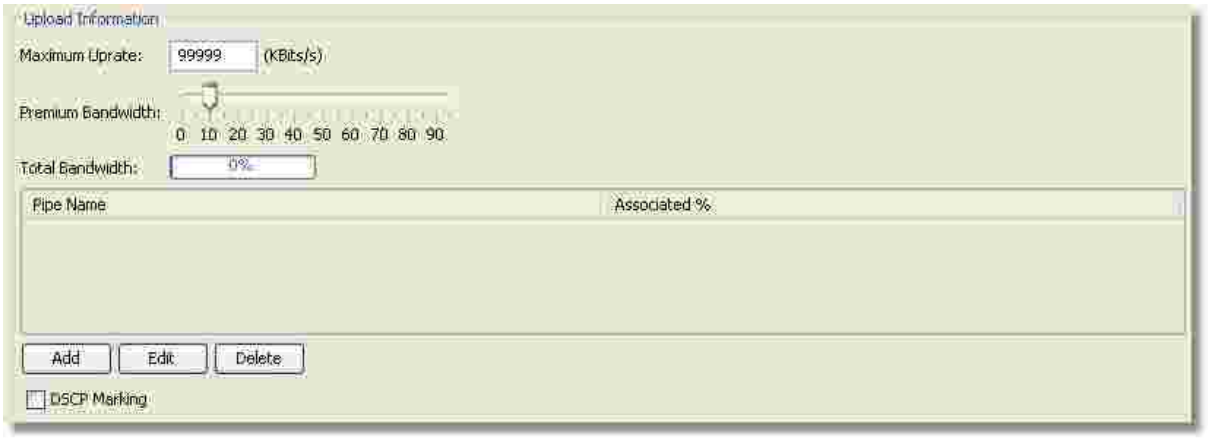
This information is read-only and provides the current status of the service. Possible values are running and stopped. This is a global setting and applies to all interfaces.

© 2006 Critical Links, SA

4.3.2 Upload Information

In this section, you can configure the QoS settings for outgoing traffic. There are four pre-defined QoS classes, each corresponding to different levels of QoS priority: upGold, upSilver, upBronze and upBE. The latter is the default QoS class, with the lowest priority. You may also reserve a percentage of bandwidth for custom classes (pipes). In the event of congestion, this percentage of bandwidth is always guaranteed for these pipes. The elements available are:

- § Maximum Uprate,
- § Premium Bandwidth and
- § DSCP Marking.



4.3.2.1 Maximum Uprate

Maximum available bandwidth for the outbound connection.

4.3.2.2 Premium Bandwidth

The bandwidth percentage reserved to upload priority traffic. You can then further subdivide this bandwidth, assigning a percentage of this bandwidth to sub connections (pipes). In case of congestion, the bandwidth is guaranteed for each of these pipes. The table present in the next panel displays the current pipes' configuration. To manage the pipe list, you have 3 operations available: “Add”, “Edit” and “Delete”.

Add

After selecting “Add”, a popup window will display. The following information will be required:

- Pipe Name: The identification for this pipe;
- Associated Percentage: The percentage of the Premium bandwidth reserved for this pipe.

After selecting “OK”, the “Total Bandwidth” indicator will be updated, reflecting the amount of premium bandwidth already used by existing pipes. You will not be able to create more pipes after this bandwidth reaches 100%. Remember to select “Apply” in the main panel for changes to become effective.

Edit

Select the pipe you want to change and then select “Edit”. A popup window similar to the one in “Add”

© 2006 Critical Links, SA

will appear, allowing you to change all the information entered. After selecting “OK”, the table will be updated, as well as the bandwidth indicator. You will not be able to make changes if the total pipes' bandwidth exceeds 100%. Remember to select “Apply” in the main panel for changes to become effective.

Delete
Select the pipe you want to delete and press “Delete”. The pipe will be removed from the list and the bandwidth indicator will be updated. Remember to select “Apply” in the main panel, for changes to become effective.

4.3.2.3 DSCP Marking

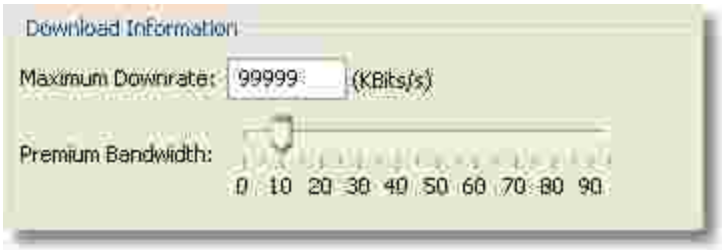
Check this box if you want packets classified and marked in accordance with the diffserv architecture. Enable this feature only if you have a QoS diffserv agreement with your ISP on the WAN side.

4.3.3 Download Information

In this section you can configure the QoS settings for incoming traffic. The elements available are described next.

Maximum Downrate
Maximum available bandwidth for the download connection.

Premium Bandwidth
Available bandwidth percentage that will be assigned to priority download traffic. In the download connection there are just two QoS classes: downBE and downPremium. Traffic belonging to the QoS class downPremium will have an amount of bandwidth reserved in case of congestion, whereas for downBE (best-effort, the default), no guarantee will be given.



© 2006 Critical Links, SA

4.4 Services QoS

Services QoS Configuration Page

This option allows you to set QoS classes to services, overriding any QoS settings for group traffic. You will be able to configure QoS classes by interface, protocol and port. You can, for example, assign a special upload class for the Internet email service, and another for your enterprise email. When you select this option, a page like the one shown above will display. You have two tabs, each corresponding to one interface: WAN and EWAN. Again the options available for each tab are quite similar, so we will just describe the settings for WAN.

In each tab corresponding to one particular interface, you have a list of the services' QoS configured. Each row lists a given configuration. Possible actions are Add, Edit and Delete.

4.4.1 Add

After selecting “Add”, a popup window will be displayed, requiring you to enter the following information:

© 2006 Critical Links, SA

Add ServiceQoS Window

- Direction: Whether the traffic is arriving from the Internet or Enterprise network – InBound or being sent across the Internet or Enterprise network – Outbound.
- QoS class: QoS class to assign to the traffic for this service;

For Outbound traffic: choose from well-known values (upBE, upBronze, upSilver, upGold) or you may also choose pipes if they were created beforehand.

For Inbound traffic: choose from downBE and downPremium.

- Protocol: Choose from the list; available options are: TCP, UDP, GRE or ESP.
- Source Address: specifies the address where the traffic originates.
- Remote Address: specifies the destination address where the traffic is delivered.

For Inbound traffic checking the Use Local Address box will specify the edgeBOX as the Remote (destination) Address.

For Outbound traffic checking the Use Local Address box will specify the edgeBOX as the Source Address.

To set the policy for all addresses enter an IP address of 0.0.0.0

- Port: The port corresponding to the service you want to configure. If the direction selected was outbound this will be the destination port; otherwise it will be the source port.

After selecting “OK”, the entry will appear in the table, for it to become effective you have to select “Apply” in the main panel.

4.4.2 Edit

Allows you to modify a services' QoS table entry. The options available for configuration are the same as for inserting a new service QoS entry.

4.4.3 Delete

After selecting a configuration from the table, select “Delete”. To make this change effective you have to select “Apply” in the main panel.

© 2006 Critical Links, SA

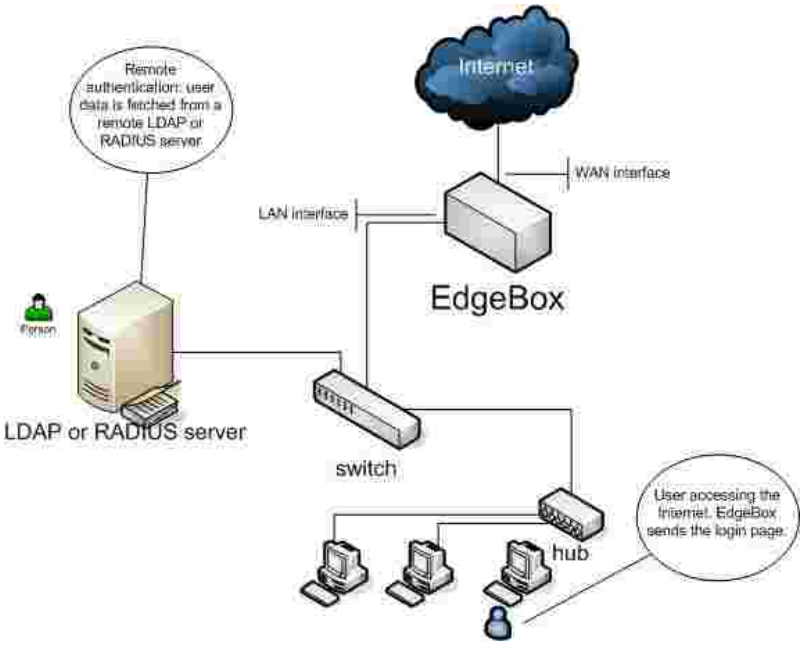
Remember that this setting overrides any QoS group configuration. For example, if you decide to assign a group an upload QoS class of upGold and configure the email service to have an upload class of upBE, then all outbound traffic from this group for the email service will be treated as upBE.

4.5 System Configuration

In this section, we will cover the options present in the System menu, namely:

- Authentication;
- Accounting;
- Date/Time;
- Syslog;
- Quota;
- Backup;
- Config;
- System Update;
- SNMP;
- Logoff.

4.5.1 Authentication



© 2006 Critical Links, SA

Possible Remote Authentication Scenario

This menu option controls the method used to authenticate users and to grant access to services. Several different scenarios are possible. User credentials may be stored locally or fetched from a remote server. This refers to authentication, i.e. the way a user proves his identity. If the user supplies the correct credentials, access to the system is granted according to a predefined policy and to those services which a user has been setup for.

Policies act at the firewall level. They define access to the Internet, to services, to the enterprise network and to VPNs.

Another concept is service authorisation. During user creation, besides ordinary user data such as username and password, the set of services a user is allowed to access is also defined. These will be the only services the user will be allowed to use. These definitions may also be stored locally or remotely.

Available configuration types are thus:

- Local Server,
- Remote LDAP Server and
- Remote Radius Server.

If you use local server authentication, user credentials will be validated against local user data. The authentication architecture has undergone major changes in edgeBOX version 4. Besides the services authorisation feature mentioned in the previous section, authentication for all services is now fully integrated, so any change in the type of authentication used will be immediately reflected in all services. For details on edgeBOX's authentication architecture, please see appendix A.

Whether you choose a local or remote authentication scheme, having credentials stored locally or remotely, a default structure is always created for each user consisting of a home directory, group policy definition, etc… When the authentication scheme used is local, this structure is created on user creation, when it is remote, the structure is created upon the user's first successful authentication.

No matter which authentication scheme is chosen, the option “Purge Existing Local Users” will always be available. This option allows you to delete all user data from edgeBOX. This is particularly important when you change the type of authentication scheme used as it prevents inconsistencies appearing. You should always select this option when changing the authentication type.

4.5.1.1 Remote RADIUS Server Authentication

If you choose “Remote Radius Server”, a table will be populated with the servers to be used

© 2006 Critical Links, SA

configured. You can use more than one server, causing them to be queried in sequence. If the first one is not available, the next will be queried until one answers. The operations available to manage the server list are “Add”, “Edit” and “Delete”.

If you check "Use for Authorisation", then service authorisation will also be performed remotely. For details on how to configure a Radius server to perform authentication and authorisation, please refer to appendix A.

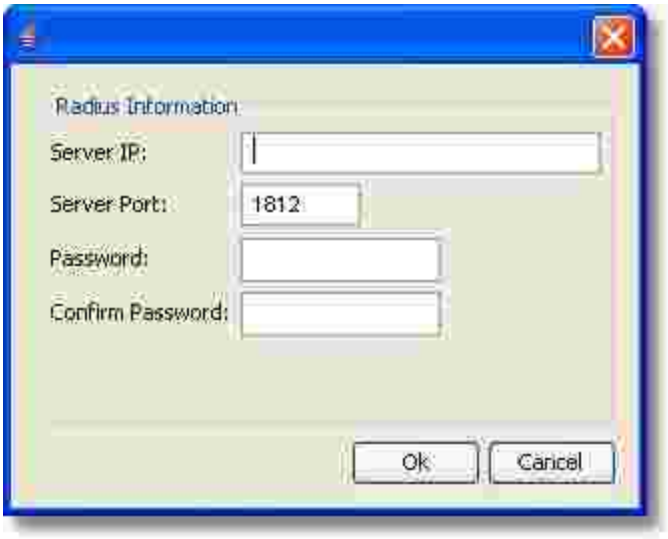
If you check "Purge Existing Local Users", then all user data currently stored on edgeBOX will be deleted.

Options available for Remote RADIUS Authentication

4.5.1.1.1 Add

Adds another server to the list. You will need to provide the following information:

© 2006 Critical Links, SA



Radius Server Information.

- Server IP: The IP address for the remote server;
- Server Port: The port used for authentication. The default port used is 1812.
- Password: The password used by edgeBOX's radius client to connect to the remote server and
- Timeout: The maximum amount of time for a valid answer from the RADIUS server. If this time is exceeded, the next server on the list (if any) will be queried.

4.5.1.1.2 Edit

After selecting the server row corresponding to the server configuration you want to change, select the “Edit” button. A popup window similar to the one in “Add” will be visible, allowing you to change the information already entered. After selecting “OK” you will have to select “Apply” in the main window for changes to become effective.

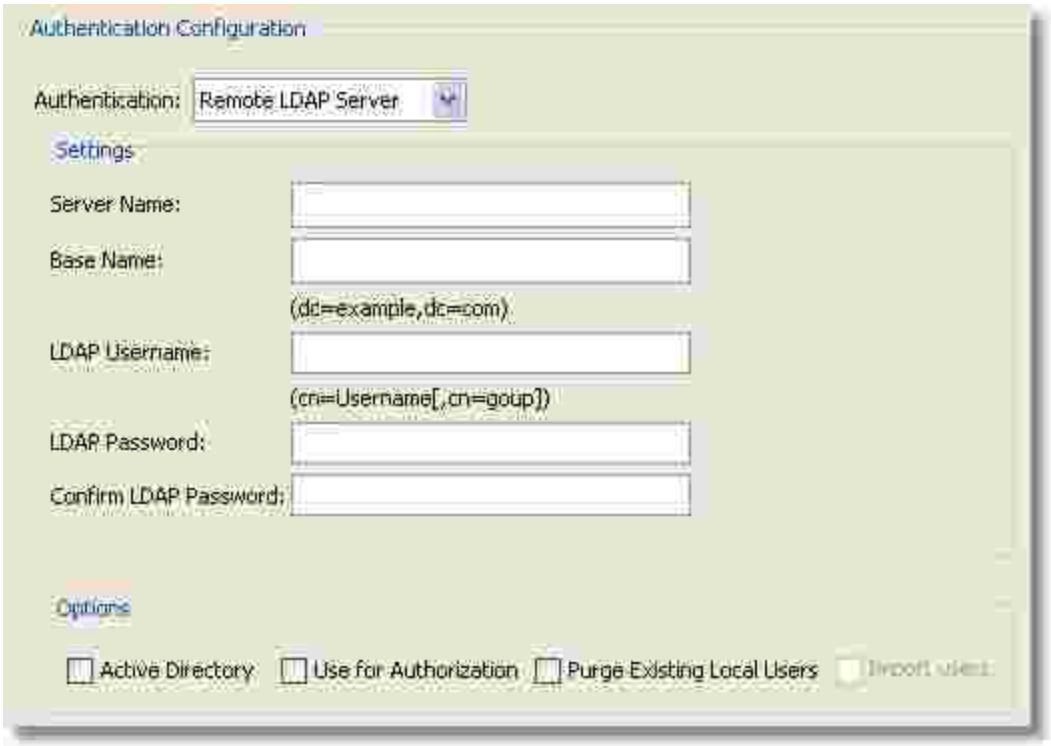
4.5.1.1.3 Delete

Removes a server from the list. After selecting the server to delete, select the “Delete” button. Remember to select “Apply” in the main panel for changes to become effective.

4.5.1.2 Remote LDAP Server Authentication

If you choose “Remote LDAP Server” the following information will be required:

© 2006 Critical Links, SA



Options available for Remote LDAP Authentication

- Server Name: The IP address for the remote LDAP server;
- Base Name: The active directory domain configured;
- LDAP Username: A username that will be used to make the LDAP binding;
- LDAP Password: The password for the above username;
- Confirm LDAP Password: Used to confirm the password supplied in the previous option.

Additionally, the following options will be available:

§ Active Directory: If you check this option, an Active Directory server will be used as a repository for credentials. The "Use for Authorisation" checkbox will be disabled and the "Import Users" checkbox will be enabled. If you check "Import Users" then all local user data will be immediately created. This is the only remote authentication scheme where this happens since all other remote schemes will do this after the user's first successful login. For more details, see appendix A.

§ Use for Authorisation: Check this option if you also want to use the remote LDAP server for service authorisation. Please refer to appendix A for details on configuring a remote LDAP server for performing authentication/authorisation. This option will not be available if you have checked "Active Directory".

§ Purge Existing Local Users: Checking this option will delete all user data stored on edgeBOX.

4.5.2 Accounting

This menu option allows you to review and configure the Radius servers used for accounting. Note

© 2006 Critical Links, SA

that you can have authentication and accounting performed by the same server, or have different servers for each purpose. The table lists all the servers configured. The configured servers will be contacted in sequence, and the first one to answer will store the data. The accounting data applies only to the WAN interface. Available actions are “Add”, “Edit” and “Delete”.

Add
After selecting “Add” a popup will display, requesting you to enter the following information:

- Server IP: The IP address for the new server;
- Server Port: The port used. The default value is 1813, but another port may be used.
- Password: The password used by edgeBOX's radius client to access the server;
- Timeout: The maximum amount of time for connection setup with the RADIUS server. If this time is exceeded then the next server on the list (if any) will be contacted.

Edit
Change the settings for a listed server. After selecting the server configuration to edit, press “Edit”. After changing the possible options and selecting “OK”, you will have to select “Apply” in the main panel to make changes effective.

Delete
Deletes a server from the list after selecting it and pressing “Delete”. You will have to select “Apply” in the main panel for changes to become effective.

Log Network Traffic
Select from the list, where possible values are “Off”, “15 minutes”, “30 minutes” and “60 minutes”. This option allows you to control the period for which account information will be recorded. If set to “Off”, traffic information will be logged only when users log off. If not, the label indicates the interval between logs: 15 minutes, 30 minutes or 60 minutes.

4.5.3 Date/Time

This menu option allows you to set edgeBOX's clock. You may also configure edgeBOX to use NTP (Network Time Protocol) and so its clock will be synchronised with a timeserver. Available options are described next.

Date
Enter the current date either by inserting the values directly or using the up-down controls.

Timezone
Select from the list of available values.

Time
Enter the current time either by inserting the values directly or using the up-down controls.

Daylight Saving Time
This option is read-only.

Use Network Time Protocol
By checking this option, the NTP protocol will be used to fetch the time from a server.

NTP Server
The server from which the time will be fetched. This list will only be available if the previous control is

© 2006 Critical Links, SA

checked.

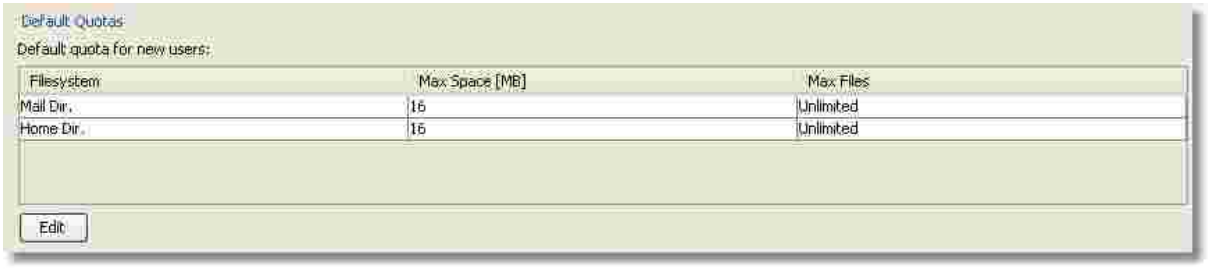
4.5.4 Syslog

This menu option allows you to configure remote logging. You need to configure a syslog server to accept connections from the edgeBOX. The available options on this page are now described.

Remote Logging
Checking this option will activate this feature.

Remote Location
The IP address for the remote syslog server to which edgeBOX will send its logs.

4.5.5 Quota



Quota Configuration Page

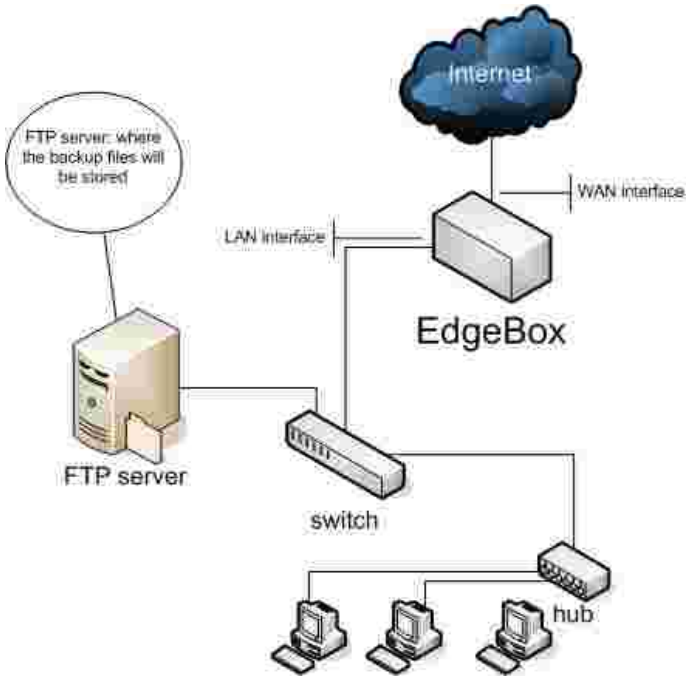
This menu option allows you to configure disk quotas. By setting disk quotas you are limiting the amount of disk space a user may consume. This feature is useful to keep disk usage at reasonable levels (and ultimately to prevent edgeBOX from running out of disk space). You have two file systems available for which you can set quotas, corresponding to the user's home directory (where their personal web page will be located) and to the user's mail. To set users' quotas for one of these file systems:

- Select the file system for which you want to set quotas.
- Select “Edit”. A popup window will appear.
- Change the desired value(s): Maximum number of Megabytes or/and Maximum number of files.

© 2006 Critical Links, SA

- Select “OK” to confirm or “Cancel” to abort changes.
- Check the status returned for errors.

4.5.6 Backup



Backup Setup Scenario

This menu option allows you to review and change your backup configuration. edgeBOX can schedule backups to occur periodically at a predefined time. These backups can be stored either on a remote FTP server or to a USB disk connected to the edgeBOX. Backups may be restored, totally or partially, at a later time (the user can choose the items to restore). We advise you to define a backup policy from the start, to prevent the loss or corruption of data. Next, we will describe how to configure automatic backups and how to perform a restore from a previous backup.

© 2006 Critical Links, SA

4.5.6.1 Backup Configuration

Backup State
Shows whether backups are scheduled or not.

Backup Type
Choose from the list. Possible values are: Standard and Config. Standard backup performs a full backup of the system, whereas a Config backup will only save the configuration files.

Backup Time
The time of the day at which backups will be performed. Enter the values directly in the fields or use the up-down controls.

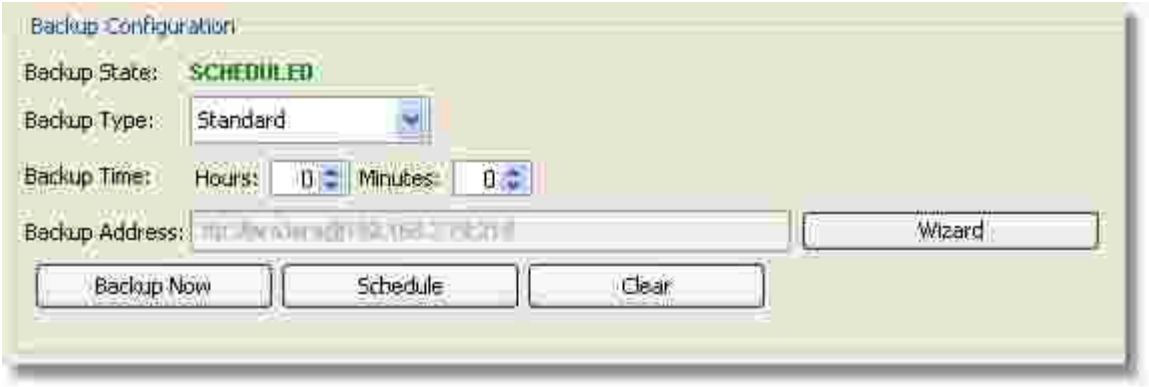
Backup Address
Specifies the destination for the backup. A Wizard is used to create the full path to the destination. A dialogue panel is displayed taking the administrator through the steps required.

For backups using FTP to a remote server the Wizard asks for: the address of the FTP server; port number (default is 21); if authentication is required, the username and password for the remote server are required, otherwise an anonymous login is used, and finally the directory on the remote server where the backup will be stored.

For backup to a local USB disk the Wizard asks for the destination disk from the devices currently connected to the edgeBOX, and the directory where the backup will be stored.

Backup Now
Immediately starts a backup of the selected type of files.

To make the previous changes effective you will have to select the “Schedule” button.



4.5.6.2 Restore Configuration

If “Activate Backup” is checked then the “Restore Configuration” panel will also be enabled providing the following options.

Note: The same Wizard is used to create the path to where the backups are stored. Backups may be restored from either a remote FTP server or from a USB disk connected to the edgeBOX.

Location
The location where the backup files are located. Clicking on the Wizard button displays a dialogue

© 2006 Critical Links, SA

panel and the Wizard will take the administrator through the steps required to create the path to the backup.

Get Info

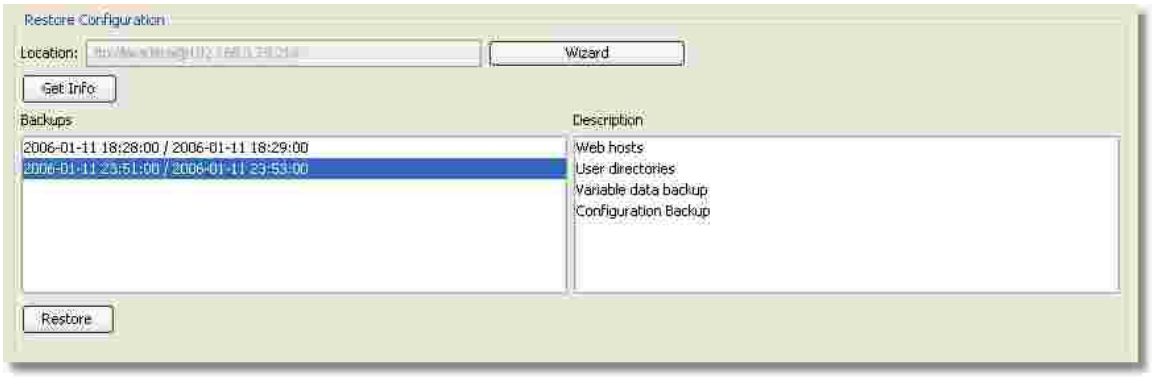
After filling these fields, selecting “Get Info” will fetch the list of available backups from the location supplied. Each row in the backups list will display the backup start time and end time. Selecting a row in the backups list will make its description appear in the list on the right.

The backup description lists the available items backed up. A standard backup will include the following items:

- Web hosts;
- User directories;
- Variable data backup and
- Configuration backup.

A configuration backup will include only the configuration data. To restore backed up data, follow the next steps:

- Fetch the list of backups from the backup server;
- Choose from the list of available backups;
- In the description list, check the item you want to restore;
- Select “Restore”.
- Check the status returned.



4.5.7 Config

This menu option allows you to configure several aspects of edgeBOX's configuration, such as the administration password, the locale, the root email, the length of time for which edgeBOX will keep logs, and also to upload SpeedTouch's firmware and to customize the landing page.

4.5.7.1 Admin Options

This option allows you to change the administration password. We strongly advise you change this password before connecting edgeBOX to any network (default values are: login admin, password root). Enter the new password in fields “New Password” and “Confirm Password” and select “Change”. Check the status returned for errors.

© 2006 Critical Links, SA

Administration Options

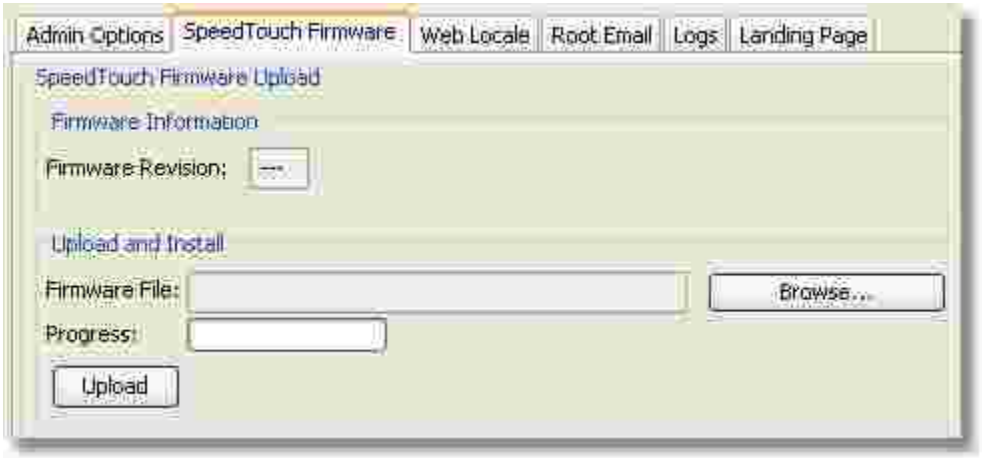
4.5.7.2 SpeedTouch Firmware

edgeBOX provides direct support for the SpeedTouch 330 USB ADSL modem. This section allows you to upload the firmware for a unit attached to the edgeBOX. You need to upload the correct firmware the first time you plug the modem into the edgeBOX.

Firmware Revision
Displays the current version number of the firmware running on a SpeedTouch modem if one is currently connected to the edgeBOX.

Firmware File
Select a file containing the firmware updates from the computer where the edgeBOX administration application is being used by clicking on the Browse button. Once selected clicking on the Upload button will upload and install the firmware on the modem.

Progress
Displays the progress of the firmware update after the Upload button is clicked.



4.5.7.3 Web Locale

The language used in the Control Centre to administer the edgeBOX can be selected.

GUI Language
Select the language used by the edgeBOX Control Centre. Currently English and Portuguese are

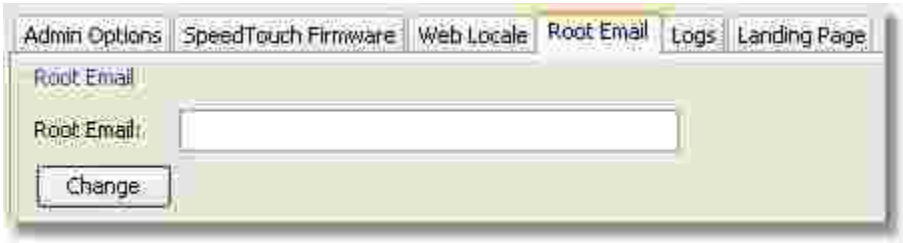
© 2006 Critical Links, SA

supported.

4.5.7.4 Root Email

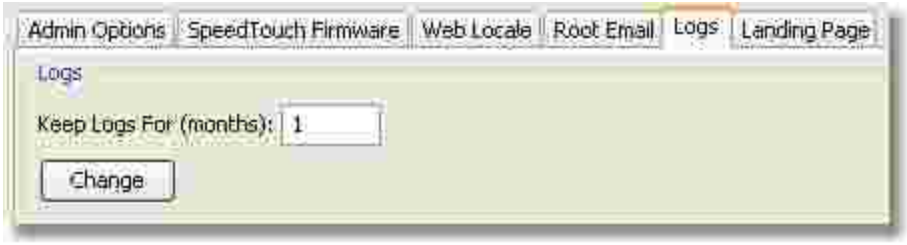
Notifications and other status messages may be sent via email to the administrator responsible for the edgeBOX. The user interface will be updated when the Change button is clicked.

Root Email
Set email address of the root user where notifications and status messages will be sent. Click on the Change button to set the email address.



4.5.7.5 Logs

Sets the amount of time log information is kept in the system. The number of months information is kept will have a direct impact on the time span of the reports produced by the reporting module. Be careful not to save too much information, or you may run out of space.



4.5.7.6 Landing Page

With this option you can customise several aspects of the login page your local network users will use to authenticate if the option "Require users to login" was checked on the Firewall panel. The following items may be configured:

Notice
This option allows you to customize the message that will appear under the login form fields. By default this message will be blank. After changing the message select the upload button to make this change permanent.

Disclaimer

© 2006 Critical Links, SA

This option allows you to customize the disclaimer text that will appear on the bottom of the page. After editing the disclaimer message select the upload button to make this change permanent.

Company Logo

This option allows you to insert your company logo. Use the Browse button to fetch the image file from your hard disk, and the upload button to store it on edgeBOX. You can check the upload progress through the progress bar.

System Network Services Security QoS Policies State Users Wizards Help
Configuration Options
Admin Options SpeedTouch Firmware Web Locale Root Email Logs Landing Page
Landing Page Configuration
Upload Text
Notice
Disclaimer
You're requested to Authenticate in order to enter 's private network. Please provide your username and password below.
If you're a employee and do not have a username and password please contact your system administrator.
If you're a visitor to and you need to access the internet, please request a guest username
Upload
Company Logo
Image File:
Browse...
Progress:
Upload
Status Information
Terminated.
edgeboxx

4.5.8 System Update

Updates are available for all software installed on edgeBOX. The updates include new functionality and performance increases for network services as well as updates to improve security and correct any vulnerability reported. There are two panels which you may use to access this functionality: System Update, where you check for and install the new updates and Configuration, where you set the configuration mode and options.

4.5.8.1 System Update

Available Updates

Displays a list of all of the updates that are currently available for edgeBOX and have not yet been installed.

System Update Log

Reports all of the updates that have been applied to edgeBOX. The list can be cleared by clicking on the Clear Update Log button.

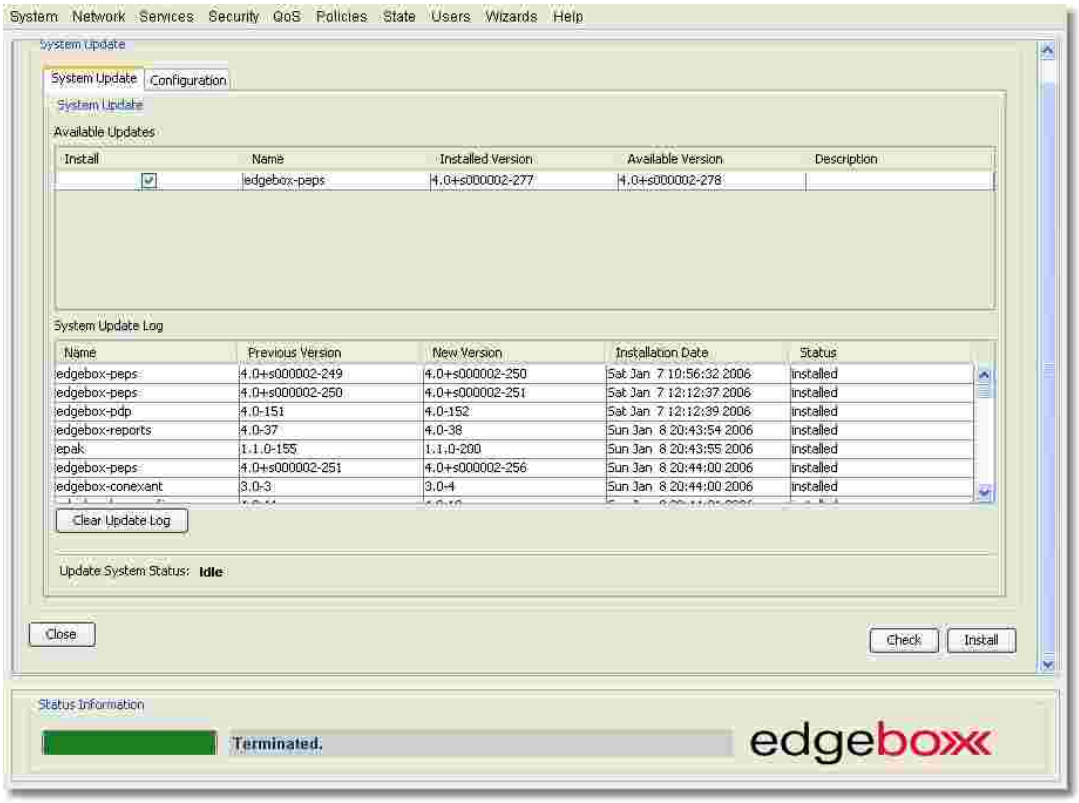
Update System Status

© 2006 Critical Links, SA

Reports the current progress of the update process - download/installation of packages.

Check
Clicking this button will immediately check for new updates. Whether the update is reported, downloaded or installed will depend on the Update model selected.

Install
Installs all the Available Updates where the Install checkbox has been checked.


System Network Services Security QoS Policies State Users Wizards Help
System Update
System Update Configuration
System Update
Available Updates
Install Name Installed Version Available Version Description
edgebox-peps 4.0+s000002-277 4.0+s000002-278
System Update Log
Name Previous Version New Version Installation Date Status
edgebox-peps 4.0+s000002-249 4.0+s000002-250 Sat Jan 7 10:56:32 2006 installed
edgebox-peps 4.0+s000002-250 4.0+s000002-251 Sat Jan 7 12:12:37 2006 installed
edgebox-pdp 4.0-151 4.0-152 Sat Jan 7 12:12:39 2006 installed
edgebox-reports 4.0-37 4.0-38 Sun Jan 8 20:43:54 2006 installed
epak 1.1.0-155 1.1.0-200 Sun Jan 8 20:43:55 2006 installed
edgebox-peps 4.0+s000002-251 4.0+s000002-256 Sun Jan 8 20:44:00 2006 installed
edgebox-conexant 3.0-3 3.0-4 Sun Jan 8 20:44:00 2006 installed
Clear Update Log
Update System Status: Idle
Close
Check
Install
Status Information
Terminated.
edgebox

4.5.8.2 Configuration

Update Mode
There are three ways to install the updates:

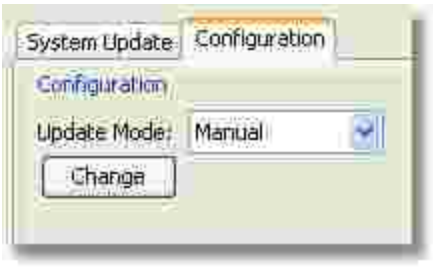
- Automatic – updates are downloaded and installed on edgeBOX without any action from an administrator except if the packages to install require either a system reboot or a service restart. In the later case, the updates must be installed manually.

- Semi-automatic – updates are downloaded to edgeBOX and an administrator selects the ones to install from the list of available updates from the System Update panel.

- Manual – the list of available updates is displayed in the System Update menu and an administrator selects which ones to download and install.

Click on the Change button to activate the selected Update mode.

© 2006 Critical Links, SA

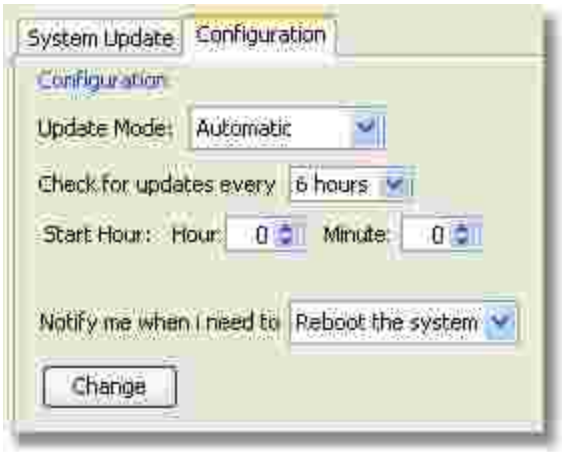


If Automatic updates are selected the following fields are presented:

Check for updates every
Sets the interval for checking whether updates are available. Choose either 6, 12 or 24 hours.

Start hour
Sets the time to begin checking for updates each day.

Notify when I need to
Some updates require either a network service to be restarted or, for more important updates, edgeBOX must be rebooted. Depending on what you choose for this item, a window will pop-up after you log on to the Control Centre, warning you there are updates available that require action after being installed.



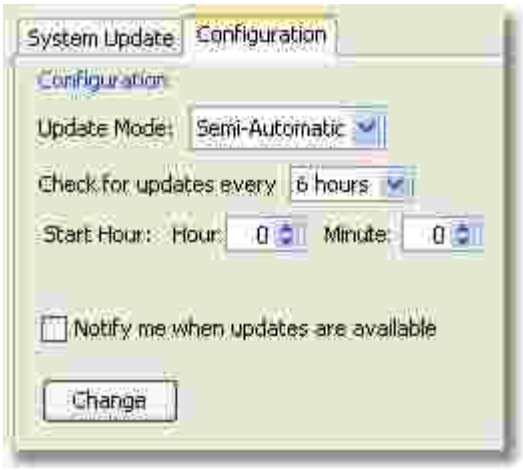
If Semi-Automatic updates are selected the following fields are presented:

Check for updates every
Sets the time interval for checking whether updates are available. Choose either 6, 12 or 24 hours.

Start hour
Sets the time to begin checking for updates each day.

Notify me when updates are available
If this box is checked, after you log on to the Control Centre a window will pop-up informing you new updates are available.

© 2006 Critical Links, SA



4.5.9 SNMP

The status of the edgeBOX can be queried using the Simple Network Management Protocol. This panel controls the SNMP agent running on the edgeBOX.

4.5.9.1 SNMP RO Configuration

Configures read-only access to the edgeBOX.

Enable RO Community

© 2006 Critical Links, SA

Enables the SNMP agent and allows read-only access to report the status of the edgeBOX.

Community
The name of the community used when requesting access to the SNMP agent. Avoid well known strings such as “public”, “private” or ones that are easy to guess, e.g. “edgebox”. Specifically “public” is not allowed.

Allow queries from
The host name or IP address of a computer which will be granted sole access to the SNMP agent. Queries from any other address will be rejected.

Restrict access below this object
Enter an object identifier (OID). Access to objects below this level, by any SNMP client, are not allowed.

4.5.9.2 SNMP Trap Configuration

Allows notifications to be sent for requests to access objects by an SNMP client.

Enable Traps
Enable notifications to be sent.

Community
The name of the community used when sending a notification.

Host to send traps to
The host name or IP address of a computer where notifications will be sent.

4.5.10 Logoff

This menu option allows you to perform the following actions: Logoff/Restart/Shutdown.

4.5.10.1 Logoff/Restart/Shutdown

After selecting one of these options, select “Confirm”. “Logoff” will only disconnect you from the web management interface; “Restart” will reboot the box, and “Shutdown” will halt the box. Remember you can also issue these commands via the CLI with the commands “system reboot” and “system shutdown”.

© 2006 Critical Links, SA

4.6 State Menu

This menu option will allow you to access edgeBOX status information and also some accounting reports, if you have selective authorization turned on. Next, we will describe the following sub-menu options:

- Users;
- Network;
- Services;
- Traffic Control;
- Accumulated History;
- Accumulated Session;
- Session Details.

4.6.1 Users

If you have selective authorisation turned on, this page will display a table with the users currently authenticated. Beside the username each entry will also display the IP and MAC addresses from which a user is connecting, and the group that they belong to.

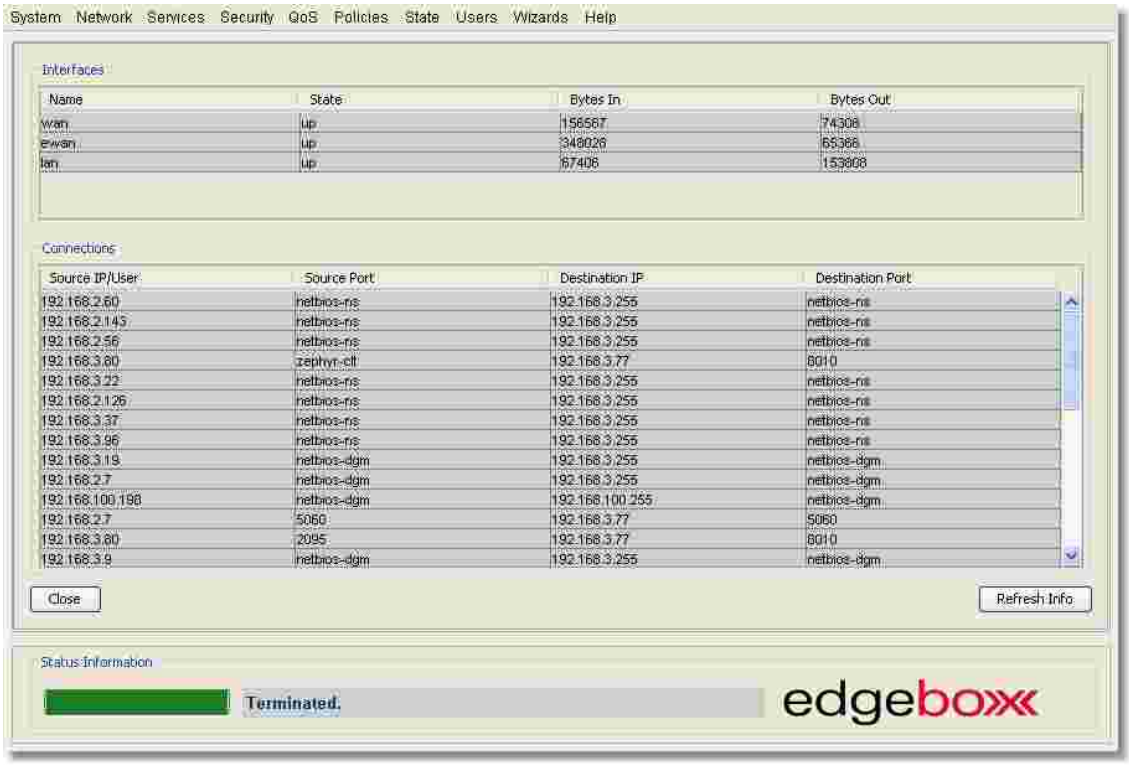
4.6.2 Network

This page will display two tables: one showing information about interfaces (the upper table) and another showing information about the connections established.

For the interfaces table, each entry will contain the following information: name, state (if it is up or down), bytes in and bytes out (for the sum of inbound and outbound bytes transferred via the interface).

For the connections table, each entry will contain the following information: source IP/user (the connection's origin – the user will be displayed only if selective authorisation is on), source port, destination IP and destination port.

© 2006 Critical Links, SA



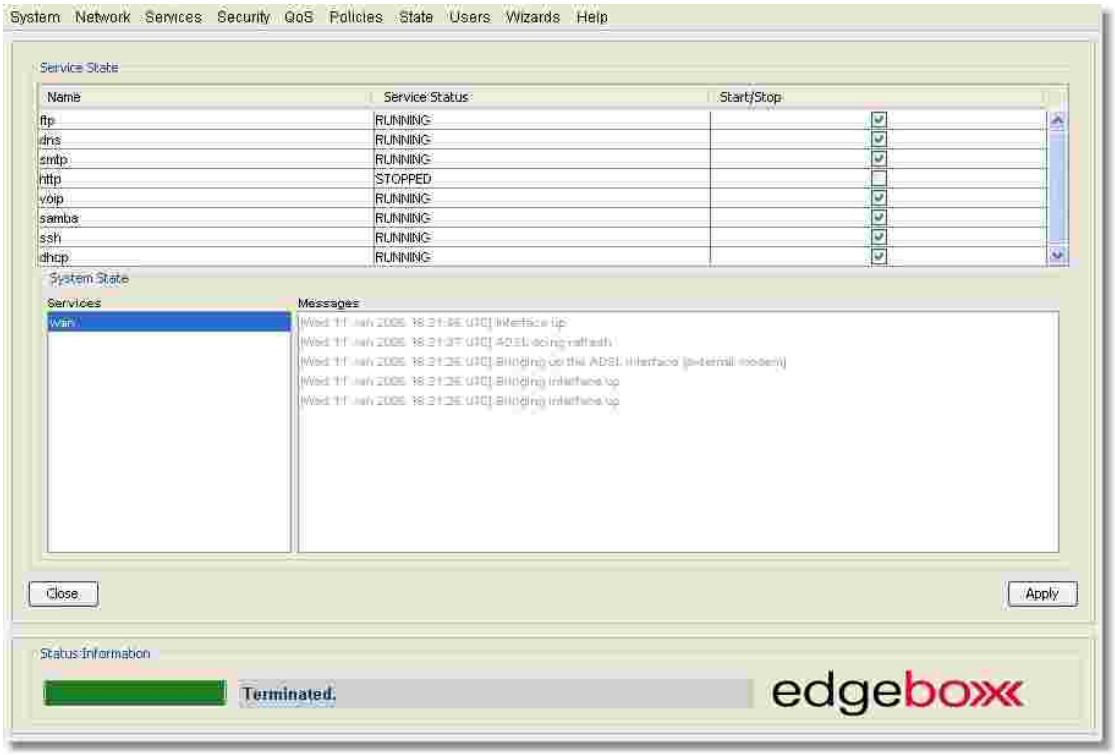
4.6.3 Services

This page will display a table with service state information. For each service line (currently the following services are listed: FTP, DNS, SMTP, HTTP, asterisk, samba and DHCP), you will have a column displaying the current service state, and a column with a check box that will allow you to change the service state.

To change the service state, proceed as follows:

- If you want to start a service, select its “Start/Stop” check box, so that a check is visible; otherwise it will be stopped;
- Select the “Apply” button.

© 2006 Critical Links, SA



4.6.4 Traffic Control

This page allows you to view traffic control statistics per interface. To see non-zero values you will have to start the traffic control service and assign traffic control classes either to groups or to services. For more information on configuring traffic control, please see Traffic Control. Each tab on this page represents an interface (currently WAN and EWAN), but the elements present in each are the same. We will describe these elements now. The statistics presented in these tab pages are based on information collected in the last 15 minutes.

Upload information

This panel displays statistics about outbound traffic. The panel contains an indicator with the percentage of bandwidth consumed, and below, a table with the following information: total bandwidth (bps), dropped packets, transmitted bytes and transmitted packets.

Download information

This panel displays statistics about inbound traffic. The panel contains an indicator with the percentage of bandwidth consumed, and below, a table with the following information: total bandwidth (bps), dropped packets, transmitted bytes and transmitted packets.

Class information

This panel contains a table with statistics by traffic control class. For each traffic control class, we have the following information: total bandwidth consumed (bps), dropped packets, transmitted bytes and transmitted packets.

© 2006 Critical Links, SA

4.6.5 Accumulated History

If you have selective user authorisation on, this page allows you to produce reports similar to the one shown below. For each day, the accumulated values for session time and traffic per interface are computed for a user. To produce a report for a specific user:

- Enter the username for the user you want to produce a report for in the “Username” field;
- Select the “Retrieve” button. A table should be visible if there is information available for the user entered.

4.6.6 Accumulated Session

In this page, you can produce a report very similar to the one in the previous option (the same fields) but this time the values shown will be the accumulated values for all sessions. No data needs to be entered here, as these values are computed for all users.

4.6.7 Session Details

In this page, you can produce reports like the one shown below. Here you will have a report displayed in tabular form for all sessions for a specific user during a specified interval.

To produce a report:

- Enter the username for whom you want to produce this report in the “Username” field;
- Enter the start date in the “From” fields, using the up-down controls or editing the field directly;

© 2006 Critical Links, SA

- Enter the end date in the “To” fields, using the up-down controls or editing the field directly;
- Select the “Retrieve” button.

After you hit the “Retrieve” button, a “Session Summary” table should be visible. A session is defined to be the time between a user login and logout, so each row will contain the start date and time (login time), IP (IP address from where the user logged in) and stop date and time (logout time). If you select an entry and hit the “View info” button, a window will pop-up, showing bandwidth usage per interface for the session.

Under the “Session Summary” table, another table should be visible displaying network traffic data. If you want to be able to access this data, don’t forget to turn the “log network traffic” option on (For more information, see Log Network Traffic under Accounting).

4.7 The CLI

Besides supporting configuration via a web interface, edgeBOX also supports a CLI (Command Line Interface). This CLI may be accessed in two different ways: the console, connecting a keyboard and a monitor directly to the box, and connecting through SSH to one of the interfaces (remember access to the service has to be granted in the firewall configuration).

The CLI supports a subset of commands, allowing you to perform basic configuration. You can check the available commands typing “help” in the command line. The commands available are:

```
dhcp      - configure LAN dhcp server
dns       - configure dns servers
domain    - show dns domain name
ewan      - configure Enterprise WAN interface
exit      - exits the program
help      - prints this screen, or help on 'command'
hostname  - set hostname
LAN       - configure LAN interface
quota     - system default quota management
route     - add/del static route
security  - firewall, nat and authentication control status
service   - service status
system    - system details
vpnserver - config pptp vpn server
WAN       - configure WAN interface
```

This is the output of the help command. The CLI supports command completion by pressing the 'tab' key, as in most shells. Typing help with the name of a command gives you the options available for that command. For example, typing 'help LAN', gives the following output:

```
eOS> help LAN
  Options:
  > LAN show
        - show current configuration -
  > LAN static ip <ipaddress/netmask>
        - set static configuration -
```

For example, if you want to configure this interface to have IP address 192.168.100.254 with a netmask 255.255.255.0, you would type:

© 2006 Critical Links, SA

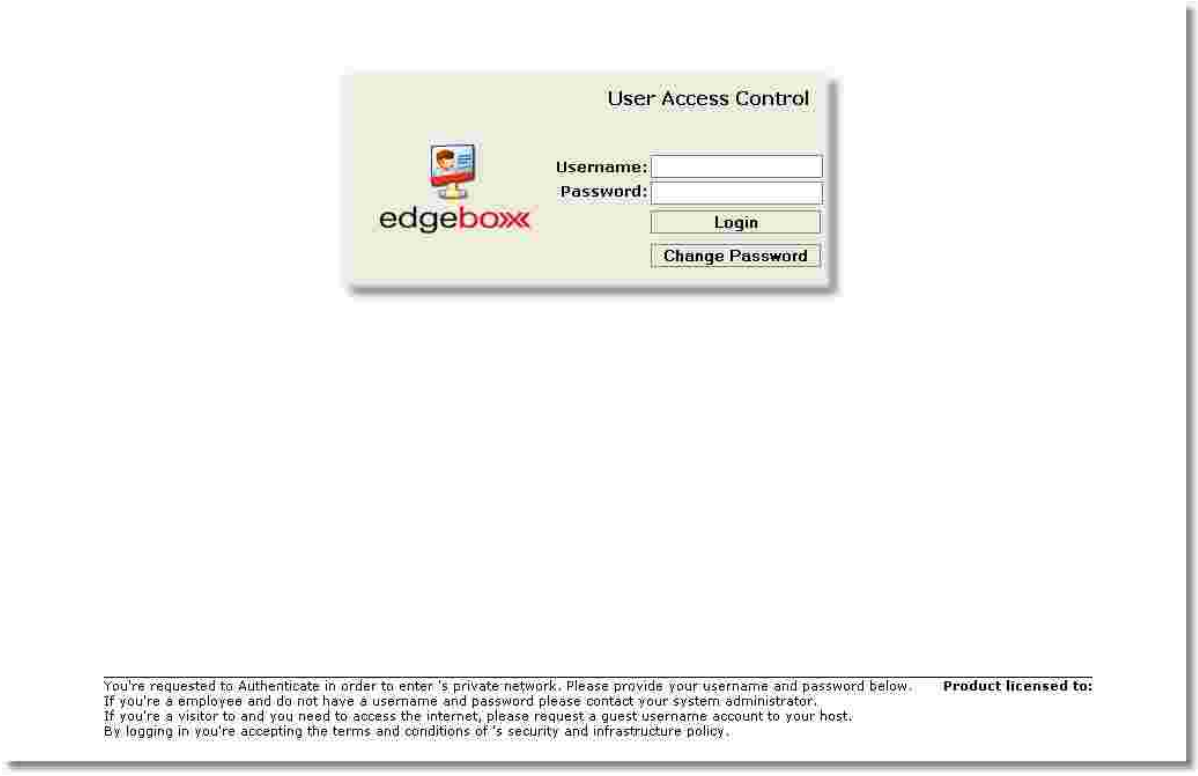
```
LAN static ip 192.168.100.254/255.255.255.0.
```

© 2006 Critical Links, SA

5 Using edgeBOX

So far we've seen how to install and setup edgeBOX. In this chapter we will show some aspects of edgeBOX's usage from an end user's point of view.

5.1 Login window


User Access Control
edgeboxx
Username:
Password:
Login
Change Password
You're requested to Authenticate in order to enter 's private network. Please provide your username and password below.
If you're a employee and do not have a username and password please contact your system administrator.
If you're a visitor to and you need to access the internet, please request a guest username account to your host.
By logging in you're accepting the terms and conditions of 's security and infrastructure policy.
Product licensed to:

Login Window

If "Require Users to Login" was checked in the Firewall panel (for more information, see Firewall Configuration), users will have to authenticate to be able to access services and resources. For example, if a client PC tries to access the Internet, a login window similar to the one above will be displayed. After entering your username and password, another popup window will be displayed, this time indicating you have successfully logged in. You must keep this window open to be able to access the network resources. If you close this window, you will be denied access and you will have to log in again.

5.2 User Data Management

So far we've used the web interface for configuring edgeBOX's services after logging in with the admin username. An ordinary user may also log in in using the same web interface, allowing them to manage their data. After logging in the user may choose one of two panels, selecting either:

- General or
- VoIP

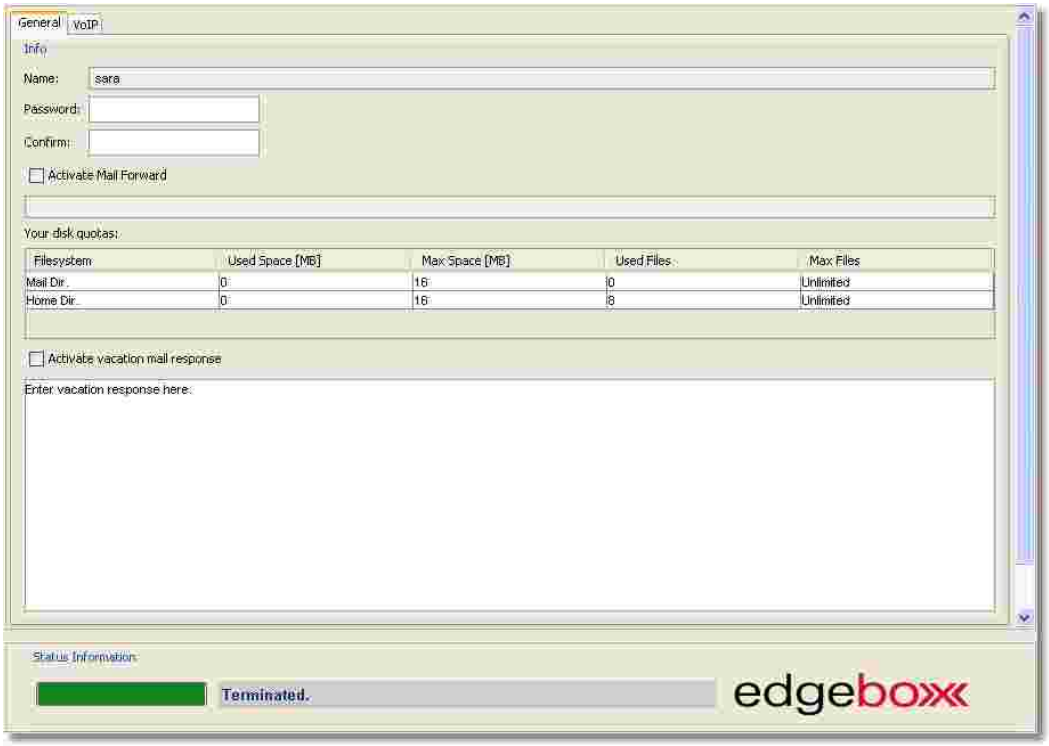
© 2006 Critical Links, SA

5.2.1 General

After selecting the "General" page, the user will be presented with a screen similar to the one in the picture below. The following options will be available:

- Name,
- Password and Confirm,
- Activate mail forward,
- Your disk quotas and
- Activate vacation mail response.

After changing any of these options, the user has to select “Apply” for changes to become effective. To leave this interface, the user may select “Logout”.



5.2.1.1 Name

This element is read-only and is the name of the user currently logged in.

5.2.1.2 Password and Confirm

These fields are used to update the user's password. If left blank, no change will be made.

5.2.1.3 Activate mail forward

If this option is checked, incoming mail for this user will be redirected to the email address entered in the field next to this option.

© 2006 Critical Links, SA

5.2.1.4 Your disk quotas

This table is included for informative purposes only – it displays the quotas configured and the space currently used by this user.

5.2.1.5 Activate vacation mail response

If you check this option, then the sender of an incoming email message for this user will receive an email with the message configured in the box that follows.

5.2.2 VoIP

This panel allows the user to configure some VoIP settings and to check voicemail messages.

5.2.2.1 Settings

This panel allows the user to configure some VoIP settings. The following options are available:

- Caller ID: the name by which calls will be identified to the called party;
- Secret: password used to register with edgeBOX.

The user will also be able to enable voicemail. By doing so, a PIN and an email address to receive notifications must be supplied.

5.2.2.2 Inbox

This panel allows the user to check the list of voicemail messages. Individual messages may be played selecting the desired message and pressing the "Play" button.

© 2006 Critical Links, SA

5.3 Web Mail

Web Mail Login Page

© 2006 Critical Links, SA

If you have the SMTP service running with a web mail domain defined (see SMTP, Email Domains), the HTTP server running and you have allowed access to it, you may access the email service through a web browser. All you have to do is point your browser to the “webmail” directory on edgeBOX's web server. For example, if edgeBOX's LAN interface is configured with address 192.168.100.254, then you should point your browser to: http://192.168.100.254/webmail.

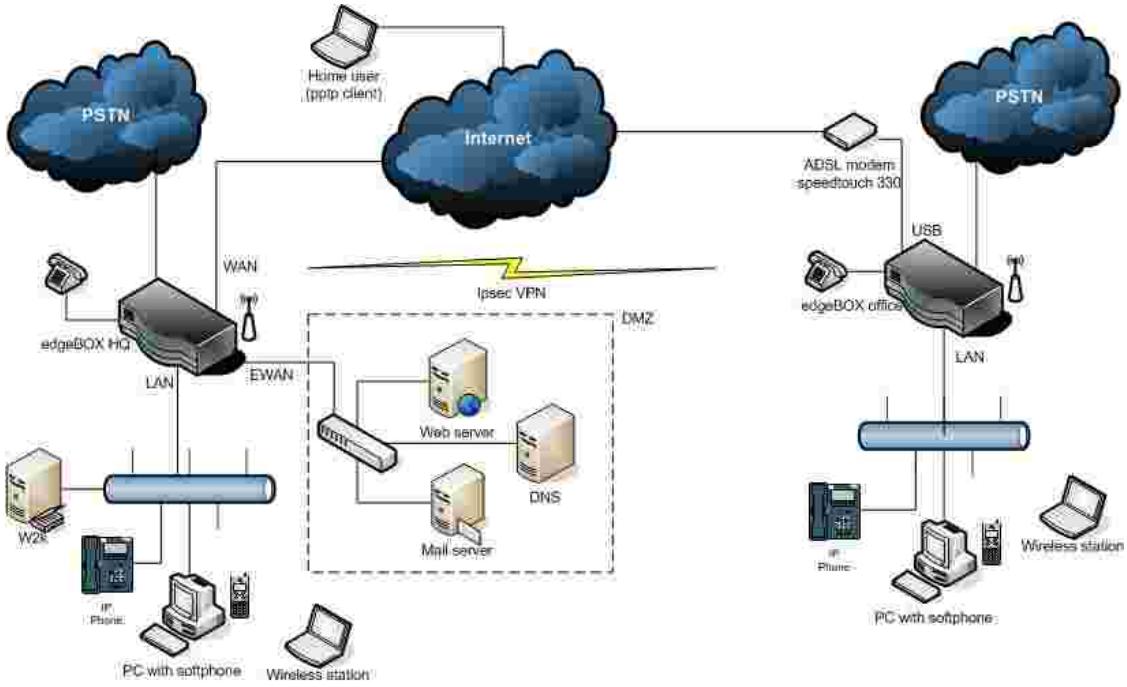
© 2006 Critical Links, SA

6 Configuration Examples

The edgeBOX can run in different types of operational modes. The mode best suitable for your situation depends on several factors including your current office network environment and Internet connection type. This section shows a complete scenario - a company's headquarters and its small remote office. Some aspects of this configuration will be dealt with separately:

- IVR configuration;
- IPsec VPN and
- Remote Switch.

The complete scenario is displayed in the picture bellow.



On the left side, it is shown the configuration for the company's headquarters while on the right the company's remote office.

Each site is connected through an IPsec tunnel. Also, a remote switch is configured between the two sites.

In the sections that follow, each site's particular requirements will be presented, as well as the guide to perform the configuration.

6.1 Scenario 1: SME branch office

The requirements for the SME branch office are the usual requirements one would expect to find for a small office:

- ADSL connection to the Internet using a dynamic configuration;

© 2006 Critical Links, SA

- Private LAN, protected by firewall but without the need for user authentication;
- Wireless access*;
- Web and SMTP servers;
- PPTP server for users connecting remotely*;
- IP PBX with the following features:
  - internal extensions, able to connect to and be accessed from the outside (pstn network);
  - voice mailbox available for people calling during off-work hours;

* these features will be common to the HQ configuration

6.1.1 Step 1: WAN connection

The WAN connection will be provided by a ADSL connection with a dynamic configuration. The modem used in this example will be the USB ADSL modem SpeedTouch 330. Perform the following actions to configure the connection:

- Follow the "Embedded firmware for Linux users" in SpeedTouch's support page to download the modem's firmware. Unzip the downloaded file contents. The firmware file is prefixed with ZZZL_.
- In Control Centre, under the System menu, choose the Config option. The configuration options panel will load;
- In this panel, choose the "SpeedTouch Firmware" tab.
- Select "Browse" to locate the firmware file.
- Select "Upload". After completion, the firmware revision loaded will be available.

After loading the firmware, you are now ready to configure the WAN interface:

- Choose the Interfaces option under the Network Menu;
- The WAN tab will be selected by default. Choose PPPoE under IP Information. Fill in the fields according to the information provided by you by your ISP.
- Check the "Internal Modem" checkbox
- Press the Apply button.

To check for interface status, reload this panel and watch the Status field.
In our scenario, we want to be able to access the the external interface by hostname so the no-ip service will be used. To do so:

- On your web browser, go to no-ip's website. Create an account and then create an host with the name branchoffice;
- In edgeBOX's Control Centre, select "Dynamic DNS", under the "Services" menu;
- Insert the following information:
  - DNS Server: No-IP;
  - Hostname: branchoffice;
  - Username/Password/Confirm Password: fill in with your credentials;

Apply your configuration. After a while, you should be able to access branchoffice.no-ip.org.

6.1.2 Step 2: LAN connection and security

Next, we are going to configure the LAN interface and the security settings. For the internal network, we can assume as this is a small office, a class C network will be enough. So, supposing the ip address for the LAN interface is 192.168.1.254, and the network address is 192.168.1.0/24, perform

© 2006 Critical Links, SA

the following actions:

- In the Control Centre, under the Network menu, choose the Interfaces option;
- In the Interfaces panel, choose the LAN tab;
- Fill in the fields with the following data:
  - IP: 192.168.1.254
  - Netmask: 255.255.255.0

Select "Apply".

Next, the hostname and internal domain will be configured. Suppose we choose "edgebox" for the hostname and "branch.local" for the internal domain:

In the same panel, select the Hostname and Domain tab;
Fill in the fields with the following information:

- Hostname: edgebox
- Domain: branch.local.

After you apply your configuration, a pop-up window will be displayed, warning you that you have to restart your edgeBOX in order for the configuration to take effect. Do so by selecting OK.
Basic connectivity is now configured. Next, we are going to make sure there's name resolution for you internal clients. To do so:

- Load the Control Centre. Login as admin and select the DNS option under the services menu;
- Under "Domain Name", select "New". A pop-up window will be displayed;
- Fill in the fields with the following information:
  - Domain Name: branch.local
  - Domain Type: Master
  - Domain Access: Internal
  - Network Address: 192.168.1.0
  - Name Server IP: 192.168.1.254

Press OK and then press "Apply". Make sure the service status is "Running". If it is not, press the "Start" button.

As the address range we have chosen for our internal network is a private one, we will have to perform network address translation, to allow our clients to access the Internet. To do so:

- Select the NAT option, under the Security menu;
- If there is an entry in the table that does not fit your needs, select it and press "Delete";
- Select "Add". A window will pop-up. Fill in the fields will the following values:
  - IP: 192.168.1.0 (your LAN network address);
  - Netmask: 255.255.255.0;
  - Interface: wan

Press "OK" and apply the changes. From this moment on, client machines on your internal network will be able to access the Internet.

Next, you may wish to configure the DHCP server to allow your LAN's client workstations to have their IP configuration fetched dynamically from edgeBOX. To do so:

- Select the "DHCP" option under the Services menu;
- If there is a range already configured and it doesn't fit your needs select it and press "Delete".

© 2006 Critical Links, SA

- In "Ranges", select "New". Enter the following information:
  - Start IP: 192.168.1.100
  - End IP: 192.168.1.200
  - Prefix: pc.

Select OK and apply your changes. Client machines with a dynamic configuration will be able to fetch all their IP configuration from edgeBOX and to connect to the Internet.

As have been said although there is the need to protect the internal network from attacks from the Internet, we will not use authentication. A good policy is to deny access to all services except those we will be providing. As such only the following services will be allowed access from the Internet: SMTP (electronic mail), SSH (secure shell), HTTP (web server) and POP3 (read mail remotely). The EWAN interface will not be connected so all services will be disabled. For the LAN interface, besides the services mentioned for the WAN interface, the following services are also allowed: DNS, VoIP, FTP and Samba. Access to the webadmin will only be allowed from the inside network. To load this configuration, follow these steps:

- Select the "Firewall" option under the menu "Security";
- Make sure the "Require users to login" option is unchecked;
- Make sure the "Enable Firewall" option is checked;
- Make sure the Wan and Ewan checkboxes in "WebAdmin Access" are unchecked;
- Check the "Select All" checkbox. All services will be allowed in all interfaces;
- Uncheck all options under the Enterprise column (EWAN);
- Uncheck all options under External, except: SMTP, SSH, HTTP and POP3;
- Uncheck all options under Internal, except: DNS, SMTP, VoIP, FTP, HTTP, POP3 and Samba.

Apply your configuration.

6.1.3 Step 3: Wireless connection

Even for a small office it is useful to be able to connect to the network using a wireless connection. The way allowed stations are managed is out of the scope of this text. We will assume WPA security will be used to avoid connections from unwanted stations. The SSID will be branchAP, the channel chosen will be 7 and we will also want our AP not to be discovered by broadcasts. To perform this configuration, do the following:

- Select "Wireless" option under the "Network" menu;
- In the "Basic" panel enter the following information:
- SSID: branchAP;
- Channel selection: 7;
- Check the "Ignore clients with broadcast SSID" checkbox;
- Check the "Allow All Clients" checkbox.
- Select the "Advanced" tab. Under "Security Type", select "WPA".
- In the panel "WPA Configuration", select "Passphrase". Enter an ascii string, for example "4444PPPP".

After entering this information, select "Apply". If the wireless status is not "Running" press the "Start" button.
Remember that client stations have to be configured according to these parameters. For details on configuring client stations to connect to edgeBOX's AP, check Appendix C.

6.1.4 Step 4: Services and users' accounts

Next, services configuration. In our scenario the requirements for a small office are:
Web server for the company only (no homepages for the users);

© 2006 Critical Links, SA

- SMTP server;
- Windows Share services for the internal LAN;
- VoIP Services (check step 6).

To configure edgeBOX for such a scenario perform the following actions:

- Login to the Control Centre. Select "HTTP" under the "Services" menu;
- Select "No" in "User Directories";
- Press "Apply". If the service state is "Stopped", press the "Start" button.

To be able to upload files to the web server you need to set a webmaster's password. To do so:

- In the same panel, enter the password for the webmaster in the "New Password" field;
- enter again the same password in the "Confirm Password" field;
- Press the "Change" button.

You can now upload files to the webserver using the webmaster username with the password entered. The files should be uploaded to the inter directory.

To setup the SMTP server do the following:

- Select "SMTP" under the "Services" menu;
- In "Email Domains" select "Add" and enter branchoffice.no-ip.org. Select "OK";
- Select "branchoffice.no-ip.org" in "Webmail Domain";
- Repeat the previous step for the branch.local domain. edgeBOX will now accept mail for both the external and internal domains.
- Select the "Access Control" tab. In "Relay Domain List" select "Add" and enter the branch.local domain. Press "OK".
- Select "Apply". If the service state is "Stopped", press the "Start" button.

To configure Windows sharing services perform the following actions:

- Select "Samba" under the "Services" menu;
- Fill in the fields with the following information:
  Workgroup: edgebox;
  Server Name: edgebox;
  Uncheck "Wins Support" and "PDC Support";
- Select "Apply". If the service state is stopped, press the "Start" button.

To be able to use these services you have to create user accounts. To create a user account, perform the following actions:

- Select "Management" under the "Users" menu;
- Press "New". Make sure the "Users" tab is selected;
- In the pop-up window that displays, enter the following information:
  Username: jdoe;
  Real Name: John Doe;
  Group: generic;
  Password: %edg7Box;
  Confirm Password: %edg7Box;
  Accesses: Check "Regular Services" and "Windows Use".

This user account will be able to fetch mail using the POP3 service using these credentials. The email account will be jdoe@branchoffice.no-ip.org or jdoe@branch.local. These credentials will also be valid when using the Windows Sharing service.

© 2006 Critical Links, SA

6.1.5 Step 5: Remote users' connection

In our scenario remote users will be able to connect to the branch office's internal network. To be able to do so the PPTP VPN server must be enabled.
To configure the PPTP VPN server perform the following actions:

- In Control Centre select "VPN PPTP" under the "Security" menu;
- Choose the range for the IPs assigned to remote clients; In Remote From enter 192.168.1.200 and in Remote To enter 192.168.1.210 (ten clients);
- Select "Apply" to commit your changes. If the service state is not running press the "Start" button.

Remote users connecting to edgeBOX's PPTP VPN server must be given proper authorisation to do so. To authorise the user created previously to connect follow these steps:

- Select "Management" under the "Users" menu;
- Select the user in the table (jdoe);
- Double click or press "Edit". The "User Edit" window will pop-up. Check the "PPTP" checkbox under "Accesses". Press "OK"

6.1.6 Step 6: VoIP features

For a small office our scenario will have the basic VoIP functionality: internal extensions, accessible from the outside and a remote switch configuration to the HQ which will be dealt with in a separate section. The extensions will also have the possibility to call the PSTN. Another interesting feature is the ability to have a voice mailbox where people calling during off-work hours can leave messages. Internal extensions can be assigned to an user upon user creation or created separately. It is not possible to assign an extension to an existing user.

To configure edgeBOX to the scenario described, we will start by creating an extension.

- In Control Centre, choose "VoIP" under the "Services" menu;
- The first panel is the phone's panel. Press the "New Phone" button;
- Enter the following information:
  Protocol: SIP;
  Extension Name: jdoe;
  Extension Number: 401;
  Password: 7625;
  Check "Active Voicemail";
  Voicemail PIN: 2333;
  Email address: jdoe@branch.local.

To illustrate how you can automatically create an extension upon user creation, create an user in the following way:

- In Control Centre, choose "Management" under "Users";
- Press "New". The "New User" creation dialog window will pop-up. Enter the following information:
  Username: voicemail
  Real Name: voicemail
  Group: generic;
  Password and Confirm Password: 4u4me
  Check the following services under accesses: VoIP;
  A VoIP panel will become available bellow. Fill in the fields with the following values:
  Extension Number: 400;
  Extension Password: 2341;
  Pin: 2131

© 2006 Critical Links, SA

Permissions: local calls.

This user was created solely with the intention of demonstrating how an extension may be created when you add an user to the system. This automatically creates an extension with the "voicemail" name. The only data that actually will be assigned to the user is the pin and the permissions (only used when authentication is used in VoIP).

So we now have two extensions: jdoe (401) and voicemail (400). Next, we are going to show how to make the extension 400 available for callers from the PSTN. For this, the IVR will be used. Perform the following actions:

- Select "VoIP" under "Services";
- Select the "Incoming Calls" tab;
- Select the ivr and press "Edit Context";
- On the panel that follows, select "Add Action";
- In the pop-up window ("New IVR Action") enter the following information:
  Select "After Press" under "Trigger Actions" and enter "401";
  Select "Dial" under "Actions";
  In "Action Parameters" select "401(jdoe)";
- Press "OK". This action will appear in the IVR tree;
- Apply the changes.

To be able to access the PSTN network, you need to configure outgoing routes. To do so:

- Select "VoIP" under "Services";
- Select the upper "Outbound Calls" tab;
- Select the "LCR" tab on your right;

On the tabs bellow you should select the type of call for which you want to define a route. Available types are Local, Long Distance, International, Mobile and Free. After selecting a type of call (for example Local) you should define the prefixes you are going to use and the route for this type of calls. If a prefix is not defined, the call will default to International.
In our simple scenario suppose we have a BRI card and no ITSPs configured. Then, the only outgoing route will be the device provided by our BRI card. It is enough to configure a route for International calls and no prefixes - this way all calls will default to International and will be routed through this device. To configure the route do the following:

- In the LCR panel, select the "International" tab;
- Under "LCR" select the route for the outgoing device in "Route". If you have a BRI card, most probably it will be mISDN/1;
- Press "Add". The route will be added to the list of routes in the tree.
- Press "Apply". You may now call the PSTN.

Finally, on our scenario we want a message to be played and a voice mailbox to be available when call arrive during off-work hours. To do so:

- Select the "Incoming Calls" tab;
- Select the "Call Rules" tab on your right;
- Press the "Add Rule" button. A dialog window will pop-up;
- Fill in the fields with the following information:
  Rule Name: Offwork;
  Select Weekdays;
  Select Monday in "From";
  Select Friday in "To";
  Select 18:00 in the "From" hours fields;
  Select 23:59 in the "To" hours fields;

© 2006 Critical Links, SA

In "Action", select "Answer". This will be the first action;
In "Action", select "Playback". Press the "Select File" button to chose a sound file. This file will be played after the call is answered;
In the window that pops-up, select an appropriate file (for example vm-intro) and press "OK";
Repeat the previous step but select the file "beep";
Change action to "Voicemail". Choose 400(voicemail);
Change action to "Playback". Choose file "vm-msgsaved";
Change action to "Playback". Choose file "vm-goodbye";
Change action to "Hangup".

- Press "OK";
- Apply your changes.

You will need to define 2 more rules like the previous one: one for the same days but for the period between 0:00 and 8:00 and on for the week-end. The time interval does not allow you to enter an interval crossing midnight.

6.2 Scenario 2: SME HQ

For the company's HQ premises, besides basic connectivity, there will be a list of additional requirements:

- Static IP and registered domain on the wan side;
- Private LAN, firewalled and requiring user authentication;
- Remote authentication, provided by the internal W2k PDC;
- Complete backups scheduled daily to the FTP server running on the W2k server;
- Email Filtering;
- DMZ with DNS, Web and Email servers;
- IP PBX with the following features:
  - Internal extensions;
  - IVR configuration with call-center and internal extensions published to the PSTN;
  - ITSP configuration;
  - Warning messages for holidays, week-ends and night hours.
  - Authentication;

6.2.1 Step 1: Wan connection

The HQ office edgeBOX will have a WAN static IP connection with a registered domain. There will be a DMZ where the DNS server will be located. Suppose you have the following configuration:

- Wan IP: 194.65.2.2/30
- Gateway: 194.65.2.1
- DNS: 212.3.24.1
- DMZ network: 212.3.24.0/29

In edgeBOX's Control Centre, do the following:

© 2006 Critical Links, SA

- Select "Interfaces" under the "Network" menu;
- In the Wan panel, enter the following information:
  IP Information: Static;
  IP: 194.65.2.2
  Netmask: 255.255.255.252
  Gateway: 194.65.2.1
  Primary DNS: 212.3.24.1
- Press "Apply".

The DMZ will be enabled later in the firewall panel. However the EWAN interface can be configured now:

In the same menu option select the EWAN tab. Enter the following information:

- IP: 212.3.24.6
- Netmask: 255.255.255.248

6.2.2 Step 2: LAN connection and Security

In the HQ scenario it is predictable that there will be a large number of machines connected to the LAN. The LAN configuration will be as follows:

- IP: 10.1.0.254
- Netmask: 255.255.0.0

In edgeBOX's Control Centre select "Interfaces" under the "Network" menu. Fill in the fields with the previous information.
Next to allow the machines to connect to the Internet we need network address translation. Do the following:

- In edgeBOX's Control Centre select "NAT" under the "Security" menu;
- Check the entries in the table; If there isn't an entry for the 10.1.0.0 network using device Wan then select "Add". A dialog window will pop-up. Enter the following information:
  IP: 10.1.0.0
  Netmask: 255.255.0.0
  Interface: wan.
- Press "OK" and then "Apply" in the main panel.
- If "NAT Enabled" is not checked, check it and select "Apply".

Next, DNS and DHCP servers are configured. Do the following:

- Select "DNS" under the "Services" menu.
- In "Domain Name" press the "New" button. A dialog window will pop-up. Enter the following information:
  Domain Name: company.internal;
  Domain Type: Master;
  Domain Access: Internal;
  Network Address: 10.1.0.0;
  Name server IP: 10.1.0.254
- Press "OK". If the status in not running, press the "Start" button.
- Select "DHCP" under the "Services" menu.
- Check if there's any range already configured. Select it and press "Delete".
- Press "New". A dialog window pops-up. Enter the following information:
  Start IP: 10.1.1.0
  End IP: 10.1.2.0
  Prefix: ws

© 2006 Critical Links, SA

- Press OK. If the status in not running, press the "Start" button.

6.2.3 Step 3: Authentication and Security

In our scenario we will enable authentication and enforce group policies. Furthermore remote authentication will be provided by a remote W2k server (although authorisation will still be local).

To configure remote authentication using a remote w2k server located at 10.1.0.1, do the following:

- Select "Authentication" under the "System" menu;
- Change "Authentication" to "Remote LDAP Server";
- Under "Settings" enter the following information:
  Server Name: 10.1.0.1;
  Base Name: dc=company,dc=internal
  LDAP Username: cn=Administrator (a user with permission to do LDAP binding);
  LDAP Password and Confirm LDAP Password: password for the user.
- Check the options "Active Directory", "Purge Existing Local Users" and "Import Users".
- Select "Apply".

Following the same policy as in the remote branch office all unnecessary services will be denied access at the firewall level.
The DNS, Email and Web servers will be placed in the DMZ. The SMTP server in edgeBOX needs to be accessible from the external network because it will receive email, perform virus scanning and forward it to the server in the DMZ. The list of services available from the external network will then be SMTP and SSH.
From the DMZ no service needs to be accessible.
The services available to LAN users will be DNS, SSH, FTP, HTTP, Voip and Samba.
To configure edgeBOX for this scenario, do the following:

- In Control Centre select the "Firewall" option under "Security".
- Check "Require users To Login" and uncheck "Ewan" and "Wan" in "Webadmin access";
- Check "Select All";
- Uncheck all services except:
- SMTP and SSH for external;
- DNS, SSH, FTP, HTTP, VoIP and Samba for internal;
- Apply your configuration

For the DMZ configuration it is not enough to perform the actual physical connections - all hosts placed in the DMZ have to be made visible. Suppose the DNS is located at 212.3.24.2, the Web server is at 212.3.24.3 and the Email server is at 212.3.24.4. Do the following:

- In the same panel, select the "DMZ" tab;
- Check "Enable DMZ";
- Press "Add". Enter the following information:
  Destination IP: 212.3.24.2
  Netmask: 255.255.255.248
  Port: 53
  Protocol: TCP
- Press "Add" again. Enter the following information:
  Destination IP: 212.3.24.3
  Netmask: 255.255.255.248
  Port: 80
  Protocol: TCP
- Press "Add" again. Enter the following information:
  Destination IP: 212.3.24.4
  Netmask: 255.255.255.248
  Port: 25
  Protocol: 25

© 2006 Critical Links, SA

- Press "Apply"

6.2.4 Step 4: Users and Group Policies

As we have said in the HQ site group policies are going to be enforced. A large set of requirements could be defined to illustrate this concept considering different types of users and permissions. Instead a small example will be given.
Consider that most of the users belong to a general group with permission to access the Internet only during lunch hours. There will be another group with will have full permissions (the administrators). Also, there will be a need for the W2k machine to have access to the Internet, since it will run the Windows update service. To build such a configuration, take the following steps:

- In the Control Centre select the "Management" option under the "Users" menu. If you followed the steps in the previous section for the authentication configuration you should see a list of users (the imported users).
- Select the "Groups" tab. You should see an entry for the generic group.
- Press "New" to create a new group. Enter "admins" in the "Group Name" field and press "OK".
- Press "New" to create a new group. Enter "servers" in the "Group Name" field and press "OK".
- Select the servers group and press "Edit". In the pop-up window select "Add IP";
- In the pop-up enter 10.1.0.1 in the "IP Address" field and press "OK". Press "OK".
- Select the "Users" tab. Edit each user and move it to the desired group. Assign the right service permissions (by default all users will have permission to use regular services);

Next we will change permissions for each group. After creation a group will not have permission to use or access any service.
To configure group permissions the way it was described earlier:

- In the Control Centre select the "Groups" option under the "Policies" menu;
- Select the generic group and press "Edit".
- Check "Allow Internet Access";
- Set the Start Hours to 12:00;
- Set the Stop Hours to 14:00;
- Check "Allow Service Access";
- Set the Start Hours to 0:00
- Set the Stop Hours to 23:59 (all day);
- Check the following services: VoIP, FTP, HTTP and Samba.
- Check "Allow Enterprise Access";
- Set the Start Hours to 0:00;
- Set the Stop Hours to 23:59;
- Check "Authorize access to VPN(s);
- Press "OK".
- Select the admins group and press "Edit";
- Check "Allow Internet Access";
- Set the Start Hours to 0:00;
- Set the Stop Hours to 23:59;
- Check "Allow Service Access";
- Set the Start Hours to 0:00;
- Set the Stop Hours to 23:59;
- Check all services;
- Check "Allow Enterprise Access";
- Set the Start Hours to 0:00;
- Set the Stop Hours to 23:59;
- Check "Authorize access to VPN(s);
- Press "OK".

© 2006 Critical Links, SA

- Select the servers group and press "Edit";
- Check "Allow Internet Access";
- Set the Start Hours to 00:00;
- Set the Stop Hours to 23:59;
- Uncheck "Allow Service Access";
- Uncheck "Allow Enterprise Access";
- Uncheck "Authorize access to VPN(s);
- Press "OK".

6.2.5 Step 5: Services

The services running on the HQ edgeBOX will be mainly accessible from the LAN. The requirements are:

- HTTP: Internal site to host the Intranet, accessible through intra.company.internal;
- SMTP: Receives mail and forwards it to the mail server on the DMZ. Sends mail from the internal hosts.
- Samba: Windows sharing service, LAN users only;
- Antivirus: Mailscanner service.

To configure edgeBOX for this scenario, do the following:

- In Control Centre select the "HTTP" option under the "Services" menu;
- Select "No" in "User Directories";
- In "Virtual Hosts" press "New";
- Select "LAN" for "Virtual Host";
- Enter "intra" in "Server Name";
- Select "Path" in "Document Root" and enter intra;
- Enter webmaster@company.internal for "Email".
- Press "OK";
- Select "Apply"
- Change the webmaster password in the same way as described in branch office.
- Select "DNS" under the "Services" menu;
- Select the company.internal domain and press "Hosts";
- Select "Add";
- In the windows that pops-up, enter the following information:
  Host name: intra;
  Host type: A;
  Host IP: 10.1.0.254;
- Press "OK". Apply the changes.

You should now be able to access the intranet site. To upload files, login with FTP as webmaster as upload files to the intra directory.
The Samba service will work in the same manner as in the branch office.
The SMTP service will be configure following these steps:

- Select "SMTP" under "Services";
- Under "Email Domain(s)" press "Add".
- Enter "company.com" and Press "OK";
- Press "Add" again. Enter "company.internal" and press "OK";
- Select "Remote" under "Storage". Enter the mail server's address: 212.3.24.4;
- Select the "Access Control" Tab. Under "Relay Domain List", press "Add";
- Enter "company.com" and press "OK";
- Press "Add" again. Enter "company.internal" and press "OK";
- Apply your changes. If the service state is stopped, press the "Start" button.

Mail sent to both domains will be received by edgeBOX, scanned for virus and forwarded to the mail

© 2006 Critical Links, SA

server located at the DMZ.
Finally, we need to enable mailscanning. Do the following:

- Select "Mailscanner" under "Security";
- Select the "Mailscanner" tab;
- Chech the "Virus scanning" checkbox;
- Choose an antivirus scanning engine. ClamAV is the only engine shipped with edgeBOX. Select it;
- Select Apply.

6.2.6 Step 6: Backups

In this scenario edgeBOX will perform a full backup to the FTP server running on the W2k server. To do so:

- In Control Centre choose "Backup" under the "System" menu;
- Enter the following information:
  Backup Type: Standard;
  Backup Time: Hours, 3; Minutes, 0;
  Backup Address: Select the wizard button. Follow the wizard and enter the following information:
    Interactive backup: FTP
    Server Address: 10.1.0.1;
    Port: 21;
    Authentication: Yes;
    Username: edgebox_backup;
    Password: a4nwq12;
    Destination directory: /;
    Press Finish;
- Select the "Schedule" button.

6.2.7 Step 7: VoIP features

In our scenario besides the common features reviewed for the branch office, such as internal extensions, call rules and LCR we need more advanced features. The need for a call centre and to be able to access internal extensions at the same time needs an advanced IVR configuration, combined with DID routes. Also, as a means to enforce call permissions to users and to avoid users from the branch office to be able to place calls though the remote switch, authentication will be used. Finally, a ITSP will be configured to demonstrate the use of LCR.

So to start with permissions enforcement we need to activate VoIP authentication. To do so:

- Select "VoIP" under "Services";
- Select the "Outbound Calls" tab;
- Select the "Authentication" tab on your right;
- Select "Authentication On". Apply your changes.

Now when users make a call to the PSTN their PIN and permissions will be verified.

Next suppose you want to contract the services of a VoIP provider to be able to lower your costs on International calls. For example, suppose you contract the voip buster service. To configure edgeBOX to use voip buster, perform the following actions:

- Select the "Outbound Calls" tab;
- Select the "VoIP Providers" tab;
- Press the "Add Provider" button. A dialog window will pop-up. Enter the following information:

© 2006 Critical Links, SA

VoIP Provider: sip.voipbuster.com
Provider Name: VoipBuster;
Username: <your username>
Password: <your password>

- Press "OK" and Apply your changes.

If you select the "LCR" tab on your right and check the "Routes" combobox, "VoIPBuster" will be available as an outgoing route.
Now a more detailed configuration will be needed - you will have to specify which prefixes match to which type of calls. As an example, consider the mobile network. In Portugal all mobile operators prefixes start with a '9'. So, to configure mobile calls to be routed to the BRI device, perform the following actions:

- Select the "Mobile" tab bellow;
- Fill in the "Prefix" field with '9' and press "Add";
- In "Route" select mISDN/1;
- Apply your changes.

Calls made to the mobile network (those starting with a '9') will be routed to the PSTN.
To route International calls through VoIP buster perform the following actions:

- Select the "International" tab;
- Fill in the "Prefix" field with '00' and press "Add";
- In "Route" select VoIPBuster;
- Apply your changes.

Two more features are needed in order to build our scenario: the sound manager and the queues. Typically you will want to upload your own sound files - you may want to translate the existing files to your own language or create new messages not found in the system files. Suppose you have a file message.gsm you want to upload to edgeBOX. Perform the following actions:

- Select the "Incoming Calls" tab;
- Select the "Sound Manager" tab on the right;
- In the "Upload Sound File" panel, press the "Browse" button. Select your sound file;
- Press the "Upload" button.

The uploaded file will now be available under "My Sound Files".
Queues are used typically in call centre scenarios, where a caller will wait other calls to be serviced until his own is answered.
Calls in queues are answered by agents so we will start by configuring an agent. Perform the following actions:

- Select the "PBX Features" tab;
- Select the "Agents" tab on the right;
- Under "Callback Login" check "Enable";
- Enter '555' in the Callback Login Extension;
- Apply your changes.

Agents will call this extension to login. After hanging up, they will be called when there is a call in a queue where they are registered. Now, to create an agent:

- In the same panel, under "Agents", press "Add Agent";
- In "Agent ID" enter a number (for example, 1);
- Enter "1111" for "PIN";
- Enter "sup1" for "Agent Name";
- Enter "201" for "Login Extension";

© 2006 Critical Links, SA

- Press "OK" and then apply your changes.

In the same manner, create agents "sup2", "fin1" and "fin2".
Now to create a queue and to assign the agents just created:

- Select the "Queues" tab on the right;
- Press "Add Queue";
- Enter "support" in "Queue Name";
- Enter "500" in "Extension";
- Select the "Agents" tab;
- Select agent "sup1". Press the "Add" button;
- Do the same with agent "sup2";
- Press the "OK" button;
- Apply your changes;

Create another queue called "financial", in extension 502 with agents "fin1" and "fin2".
These queues will be needed when the IVR configuration is reviewed.

6.3 IVR configuration

In our scenario we want to be able to access the internal extensions from the PSTN in the same manner as in the branch office configuration, and also to be able to offer a call-centre service. It is not yet possible to have two IVRs, so this have to be accomplished by other means - we will use a combination of DID routes with call rules and a more complex IVR tree.
All PBX features can be included in the IVR but in our example we are going to use only the queues configured previously (support and financial).
The way our scenario is going to be built is quite simple:

- The IVR tree will have two child nodes, ivr1 and ivr2. The first one will be a context like the one in the branch office, allowing access to the internal extensions. The second one will implement the call-centre.
- A DID route will be created with a phone number. Dialing this phone number will allow us to enter the ivr2 branch, corresponding to the call-centre. This rule will have precedence;
- The default Call rule will not enter the IVR root but the ivr1 context instead. This way the internal extensions will be available and off-work hours rules will apply.

Let's start with the IVR configuration. For simplicity sake's, we will not implement a full call-centre but just the menu entries to join the queues. To build the configuration, do the following:

- Select the "Incoming Calls" tab;
- Select "ivr" and press "Edit Context". A panel with the ivr tree is displayed;
- Press the "Add Action" button;
- Select "After Press" and enter "1" (notice this is irrelevant as this action will never happen);
- Under "Actions" select "Goto" in "Action";
- In "Select Context", select "New Context". Enter "ivr1.
- Repeat the previous step, creating an "ivr2" context.
- Press "OK" and apply your changes.

The actions and contexts should be visible on the IVR tree. We are going to assume the ivr1 tree will be configured in the same manner as we did on the branch office, so now we will edit ivr2:

- In the IVR tree, select ivr2;
- Press the "Edit Context" button;
- Press the "Add Action" button;
- Select "On Start";

© 2006 Critical Links, SA

- Under "Actions" select "Background" in "Action";
- Press the "Select File" to select a sound file. This is be typically a file with the menu entries (1 for financial, 2 for support);
- Press the "Add Action" button;
- Select "After Press" and enter "1";
- Under "Actions" select "GoTo" in "Actions";
- Select "New Context" and enter "support";
- Following the same steps, create another context this time named "financial";
- Press "OK" and then apply your changes.

So now we have two more child nodes under ivr2: support and financial. We will now edit the support context.

- Select support;
- Press the "Edit Context" button;
- Press the "Add Action" button;
- Select "On Start";
- Under "Actions" select "Background" in "Action";
- Press the "Select File" to select a sound file. This is be typically a file with some information and stating that an operator is available upon pressing "1";
- Press "OK";
- Press "Add Action";
- Select "After Press" and enter "1";
- Under "Actions" select "Queue" in "Action";
- In "Queue Name", select "support";
- Press "OK" and apply your changes.
- Perform similar actions to build the financial tree.

We now have the ivr2 tree. An user entering this tree will access the support queue pressing "1" twice. Notice we used the background action, which will not wait until the end of the sound file. Notice also that other actions could be added to make these menus more friendly. For example, a Timeout action to repeat the message; An After Press action allowing you to return to the previous menu, etc. The possibilities are endless.

Now we need to create a DID route to allow callers to enter directly in the ivr2 tree. To do so:

- Select "DID Routes";
- Press the "New Route" button;
- On number enter the number for your call centre;
- Select "Goto" in "Action" and ivr2;
- Press the "Add" button;
- Press "OK" and apply your changes.

If this number is called ivr2 will be called, placing us in the call centre tree.
Next we need to provide an entry point to ivr1 (to be able to call internal extensions). Do the following:

- Select the "Incoming Calls" tab;
- Select the "Call Rules" tab on the right;
- Select the existing rule;
- Press "Edit Rule". The "Edit Incoming Rule" dialog window pops-up;
- Under "Tree Actions" select ivr and press "Remove";
- In "Action" select GoTo. Select ivr1 and press "Add";
- Select "Goto: ivr1" in the actions' tree and use the "Up" and "Down" button to place the action in the appropriate position;
- Press "OK";

© 2006 Critical Links, SA

- Apply your changes.

This concludes our scenario.

6.4 IPsec VPN

In our scenario we want to provide a connection between the internal LANs of each site. This could be accomplished using the EWAN interface. However that would require a separate line. Another way of connecting the LANs is by using an IPsec VPN tunnel. By doing so traffic between LANs is tunneled through the Internet. The disadvantage is that the required encryption will place an additional overhead in the connection.
Suppose then the following requirements:

- Computers in the HQs site need to access all computers in the remote office;
- Computers in the branch office will need to access all computers in the HQs site;
- All services in each edgeBOX must be available to computers on the other site.

These are very generic requirements. Accesses can be fine-tuned to exclude either machines to be visible from the other site or machines not to be able to use the VPN at all.
To configure a VPN between the two sites, perform the following actions:

- In the Control Centre of the HQ's edgeBOX, select the "IPsec VPN" option under the "Security" menu. A window will pop-up.
- Enter the following information:
  Choose "Network";
  Check the "Start on system boot" checkbox;
  Tunnel Name: branchtunnel;
  Remote Network: 192.168.1.0 (this will be the remote LAN's address);
  Remote Netmask: 255.255.255.0;
  Remote Gateway: branchoffice.no-ip.org (remote office WAN address or hostname);
  Pre-shared key: 12222221;
- Select the "Services Access" tab. Check all services.
- Select the "Host" tab. Under "Local Hosts Visible to External Hosts" press the "Add" button, and enter the following information:
  Origin: 10.1.0.0;
  Netmask: 255.255.0.0;
  Protocol: ALL
  Leave the table "Local Hosts Denied..." blank.

Press "OK". Start the service if it isn't started yet.
You will then need to configure this tunnel on the remote edgeBOX. To do so:

- In the Control Centre of the remote office's edgeBOX, select the "IPsec VPN" option under the "Security" menu. A window will pop-up. Enter the following information:
  Choose "Network";
  Check the "Start on system boot" checkbox;
  Tunnel Name: hqtunnel;
  Remote Network: 10.1.0.0;
  Remote Netmask: 255.255.0.0;
  Remote Gateway: edgebox.company.com;
  Pre-shared key: 12222221;
- Select the "Services Access" tab, Check all services.
- Select the "Host" tab. Under "Local Hosts Visible to External Hosts", press the "Add" button, and enter the following information:
  Origin: 192.168.1.0;

© 2006 Critical Links, SA

Netmask: 255.255.255.0;
Protocol: ALL;

Press "OK". Start the service if it isn't started yet.
Reload the IPsec VPN's panel. When the tunnel is established, it will appear in the "Active Tunnels" table. To test it, try to ping a machine on the other site.
It may be useful to access the machines by name instead of IP address. You can configure a Forward domain in each DNS server. To do so:

- In the HQ's Control Centre select DNS under the Services menu;
- Press the "New" button under "Domain Name". The "Domain Information" window will pop-up;
- Enter the following information:
  Domain Name: branch.local;
  Domain Type: Forward;
  Domain Access: Internal;
  Network Address: 192.168.1.0;
  Name Server IP: 192.168.1.254;
- Press "OK" and then "Apply" in the main panel.
- In the branch office's Control Centre perform the same action. Enter the following information:
  Domain Name: company.internal;
  Domain Type: Forward;
  Domain Access: Internal;
  Network Address: 10.1.0.0;
  Name Server IP: 10.1.0.254;
- Press "OK" and then "Apply" in the main panel.

6.5 Remote Switch

To allow for calls between internal extensions on the company's headquarters office and internal extensions on the remote office, an IAX trunk may be configured between sites. All the other PBX functionalities will also be available.

To configure an IAX trunk between the two sites, you will have to modify the configurations on both of their edgeBOXes. So, on the headquarters' edgeBOX, perform the following actions:

Under the VoIP panel, select the "Outbound Calls" tab. On the prefix panel (the first tab on the left) select '6' for the remote switch prefix. All calls to a remote switch will start with this prefix;
Select the forth tab on the right ("Remote Switch"). The remote switch panel will be displayed;
Select "Add" to add a new remote switch. The "New Remote Switch" pop-up window will display.
Enter the following information:

- Prefix: 7;
- Name: rshqbranch;
- Secret: not4u2know
- host: branchoffice.no-ip.org
- check the "Allow Incoming Calls" checkbox
- select the gsm codec.

Select the OK button, and Apply your changes. Next, the same configuration must be performed at the remote site. The only difference here is that on host, you should enter the headquarter's office

© 2006 Critical Links, SA

hostname (edgebox.company.com). So, for simplicity, we will assume the same prefixes on the remote site. The information entered when adding a new remote switch on the remote site's edgebox will then be:

- Prefix: 7;
- Name: rshqbranch;
- Secret: not4u2know
- host: edgebox.company.com
- check the "Allow Incoming Calls" checkbox
- select the gsm codec.

At least on of the "Allow Incoming Calls" checkbox must be checked in order to allow calls to be made between sites. If by some reason you wish to restrict access to one of the sites, uncheck this checkbox on the sites' configuration.
In this scenario the sites will be connected through the Internet, so the gsm codec was chosen (uses less bandwidth).

To test this configuration, you can call an extension on the remote site. Suppose there is a remote 400 extension, dialing 67400 will allow you to call it.

© 2006 Critical Links, SA

7 Services

On the initial page, besides ‘Administration’ and ‘Reports’, you will find a third option: ‘Services’. This option was mentioned briefly in Boxes (Virtual Public Safe). We will now see how it works in detail.

Please note this option will only be available for users connected through the LAN interface. Also, the HTTP and the Samba services must be running.

After following the ‘Services’ link on the initial page, you will enter the services page where the following options are available: Main menu, Public Safes and Ewan Certificate.

7.1 Main Menu

This option will take you back to the services initial page, where some information is displayed about the operations available.

7.2 Public Safes

Every user may configure a temporary storage space which will be available for a limited interval of time. The administrator initially configures the maximum space and time available using the Samba panel in the control centre, thus activating this feature. This page may then be used to create the safes.

After choosing this option, the list of existing safes will be displayed showing the remaining time active. The options available are create a new safe, remove a safe and go back.

Create a new safe

You will be asked to choose the size and the time the safe will be active. These values are limited by the values entered by the administrator. After confirming the values, the username and password for accessing the safe will be displayed on the screen. You will then be able to access the safe in the same way you access a share.

Remove safe

In the existing safes listing, there will be a link which will allow you to remove a safe before it is automatically deleted by the system. You will have to supply the username and passwords used to access the safe.

7.3 EWAN Certificate

Choosing this option will display the EWAN certificate on the screen.

© 2006 Critical Links, SA

8 Reporting

The reporting module can be accessed from the initial page, following the “Reports” link . If you haven’t yet authenticated in the system, you will be asked to submit your credentials.
After entering the reporting module, it is possible to check the available reports and choose the one to view.

8.1 System Usage

The reports in this group show information about edgeBOX’s system usage. It is possible to export them in pdf format.

8.1.1 CPU

This report shows CPU usage in percentage, per type of process: user’s process, system processes, IO Wait processes and idle. This information is displayed in graphical and table format.

8.1.2 Load

This report shows the system load in the past 12 hours, presenting the number of active processes in both graphical and tabular format. The values for ‘Load Average (1)’ (active processes in one minute), ‘Load Average (5)’ (active processes in 5 minutes) and ‘Load Average (15)’ (active processes 15 minutes) are displayed.

As a reference, it is assumed that values bellow 1 represent good CPU load; values between 3 and 4 require close monitoring and values around 5 and 6 require immediate action because the CPU is extremely overloaded.

8.1.3 Memory

This report shows the memory usage in the past 12 hours, both in graphical and tabular format. The values of both used and free memory are presented in bytes.

8.1.4 Network Received (bytes)

This report shows the traffic received by the box at the interfaces – WAN, LAN and EWAN – in bytes per second. This information is presented in graphical format. You are able to define the time frame for these statistics: last 24h, last week or last month. To do this, select the desired option in the radio button and press ‘Search’ to generate the corresponding graphic.

You can also generate a table with the average received traffic (bytes/s) per day and per physical

© 2006 Critical Links, SA

interface. Here, ‘br0’ stands for the LAN interface, ‘imq’ stands for the intermediate queuing interface, 'eth2' stands for EWan interface, ‘eth0’ stands for WAN interface, ‘lo’ stands for the Loop back interface and ‘wlan’ or ‘ath0’ (depending on the specific wireless card used) stands for Wireless interface. ‘eth‘ interfaces assume the form 'ethn', where n’ can be 0, 1, 2 or 3 depending on the number of Ethernet cards in edgeBOX.

8.1.5 Network Transmitted (bytes)

This report shows the traffic transmitted by the box at the interfaces – WAN, LAN and EWAN – in bytes per second. This information is presented in graphical format. You are able to define the time frame for these statistics: last 24h, last week or last month. To do this, select the desired option in the radio button and press ‘Search’ to generate the corresponding graphic.

You can also generate a table with the average received traffic (bytes/s) per day and per physical interface. Here, ‘br0’ stands for the LAN interface, ‘imq’ stands for the intermediate queuing interface, 'eth2' stands for EWan interface, ‘eth0’ stands for WAN interface, ‘lo’ stands for the Loop back interface and ‘wlan’ or ‘ath0’ (depending on the specific wireless card used) stands for Wireless interface. ‘eth‘ interfaces assume the form 'ethn', where n’ can be 0, 1, 2 or 3 depending on the number of Ethernet cards in edgeBOX.

8.1.6 Network Received (packets)

This report shows the traffic received by the box at the several– WAN, LAN and EWAN – in packets per second.This information is presented in graphical format. You are able to define the time frame for these statistics: last 24h, last week or last month. To do this, select the desired option in the radio button and press ‘Search’ to generate the corresponding graphic.

You can also generate a table with the average received traffic (bytes/s) per day and per physical interface. Here, ‘br0’ stands for the LAN interface, ‘imq’ stands for the intermediate queuing interface, 'eth2' stands for EWan interface, ‘eth0’ stands for WAN interface, ‘lo’ stands for the Loop back interface and ‘wlan’ or ‘ath0’ (depending on the specific wireless card used) stands for Wireless interface. ‘eth‘ interfaces assume the form 'ethn', where n’ can be 0, 1, 2 or 3 depending on the number of Ethernet cards in edgeBOX.

8.1.7 Network Transmitted (packets)

This report shows the traffic transmitted by the box at the interfaces – WAN, LAN and EWAN – in packets per second. This information is presented in graphical format. You are able to define the time frame for these statistics: last 24h, last week or last month. To do this, select the desired option in the radio button and press ‘Search’ to generate the corresponding graphic.

You can also generate a table with the average received traffic (bytes/s) per day and per physical interface. Here, ‘br0’ stands for the LAN interface, ‘imq’ stands for the intermediate queuing interface, 'eth2' stands for EWan interface, ‘eth0’ stands for WAN interface, ‘lo’ stands for the Loop back interface and ‘wlan’ or ‘ath0’ (depending on the specific wireless card used) stands for Wireless interface. ‘eth‘ interfaces assume the form 'ethn', where n’ can be 0, 1, 2 or 3 depending on the number of Ethernet cards in edgeBOX.

8.2 Web Server

The reports in this group show information about edgeBOX’s web server usage. It is possible to export them in pdf format.

8.2.1 Status

This report shows the number of occurrences of the several possible statuses of the web server (Apache). You can choose the type of graph to see (Pie 3D, Pie 2D or line) by clicking the radio button.

© 2006 Critical Links, SA

This information is also presented in tabular format, listing the statuses and the respective number of occurrences. You can see, for example, the number of occurrences of the status 404, indicating the number of times someone tried to access a page that doesn't exist.

8.2.2 Request

This report shows the number of occurrences of the request types made to the web server (Apache). You can choose the type of graph to see (Pie 3D, Pie 2D or line) by clicking the radio button.

This information is also presented in tabular format, listing the request types and the respective number of occurrences. You can see, for example, the number of occurrences of the request 'get', indicating the number of times someone retrieved data from the web server.

8.2.3 Host

This report shows the number of times pages hosted on the web server (Apache) have been accessed. You can choose the type of graph to see (Pie 3D, Pie 2D or line) by clicking the radio button.

This information is also presented in tabular format, listing the hosted pages ('Host') and the respective number of occurrences.

8.2.4 Agent

This report shows the number of requests made to the web server by user-agent. You can choose the type of graph to see (Pie 3D, Pie 2D or line) by clicking the radio button.

This information is also presented in tabular format. You can see the number of requests (number of occurrences) made by each operation system/browser. For example, you can see that the Windows 2003/Firefox made six requests to the agent.

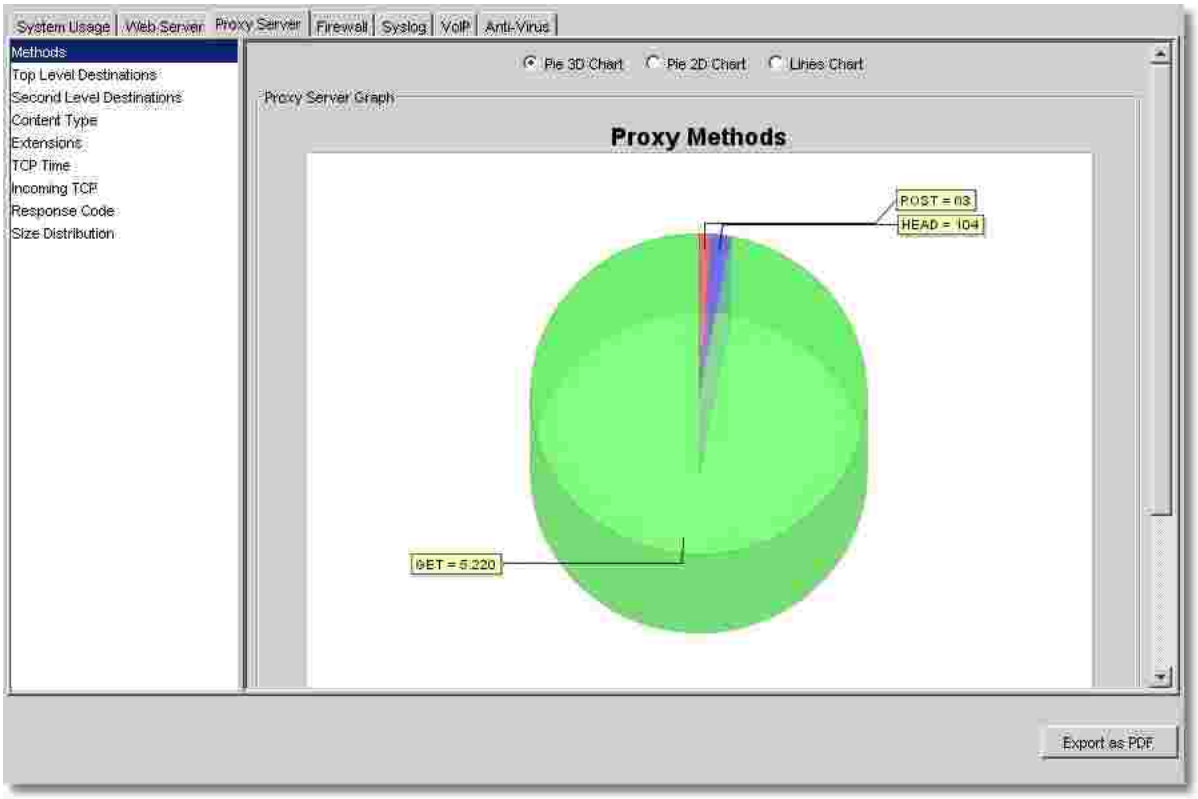
8.3 Proxy Server

The reports in this group show information about edgeBOX's Proxy Server usage. It is possible to export them in pdf format.

8.3.1 Methods

This report shows the number of occurrences of each type of HTTP method that passed through the proxy server to the web server. It is possible to select the type of graphic (Pie 3D, Pie 2D or line) by clicking the radio button.
This information is also presented in tabular format. You can check the number of occurrences for each type of method ('get', 'post', 'head', 'options' and 'propfind'). For example you can see that the method 'get' had 356 occurrences.
For a complete list of methods, please check Request methods.

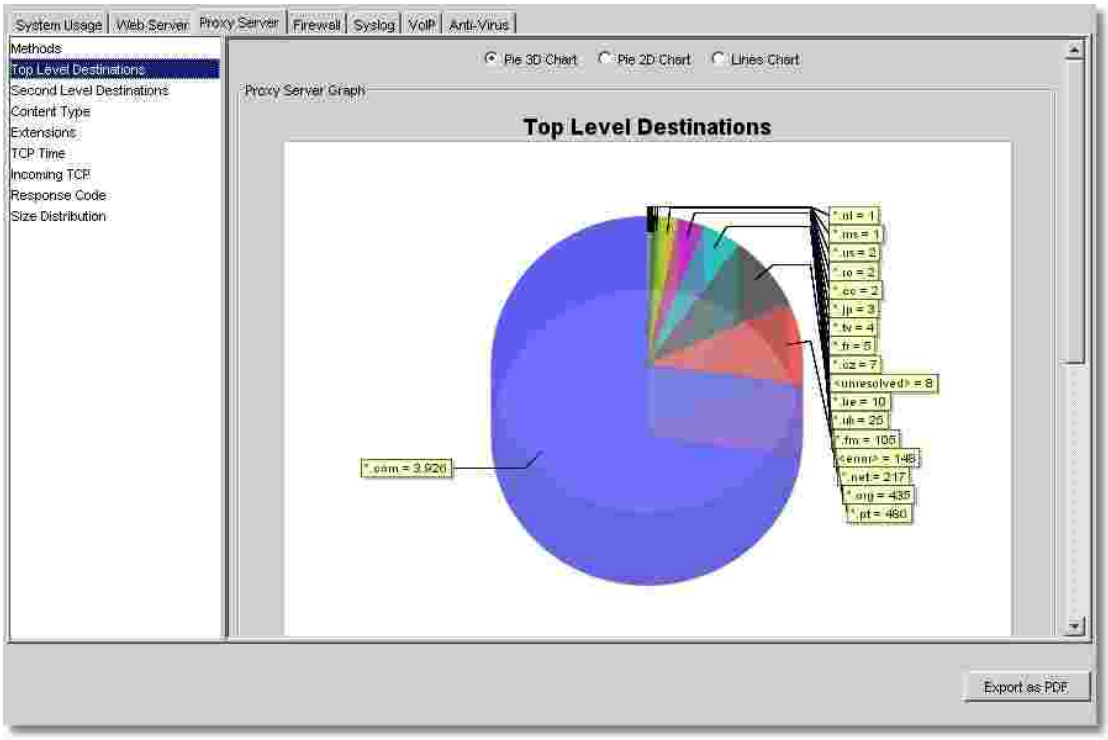
© 2006 Critical Links, SA



8.3.2 Top Level Destinations

This report shows the number of occurrences of the top level destination web pages accessed by LAN users, grouped by domain extension (for example: .com, .net, …). It is possible to choose the type of graphic (Pie 3D, Pie 2D or line) by clicking the radio button. This information is also shown in table format.

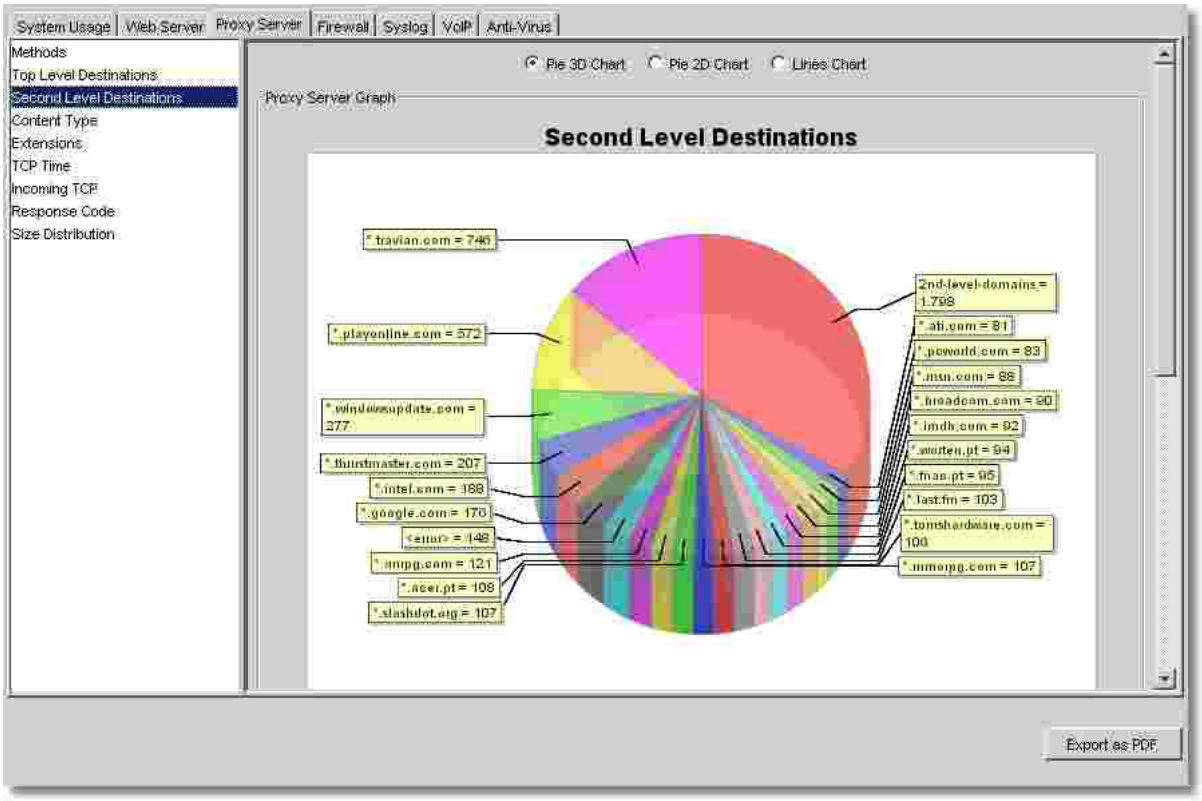
© 2006 Critical Links, SA



8.3.3 Second Level Destinations

This report shows the number of occurrences of the second level destination web pages accessed by LAN users, grouped by domain (for example: critical.com, edgebox.net, …). It is possible to choose the type of graphic (Pie 3D, Pie 2D or line) by clicking the radio button. This information is also shown in tabular format.

© 2006 Critical Links, SA



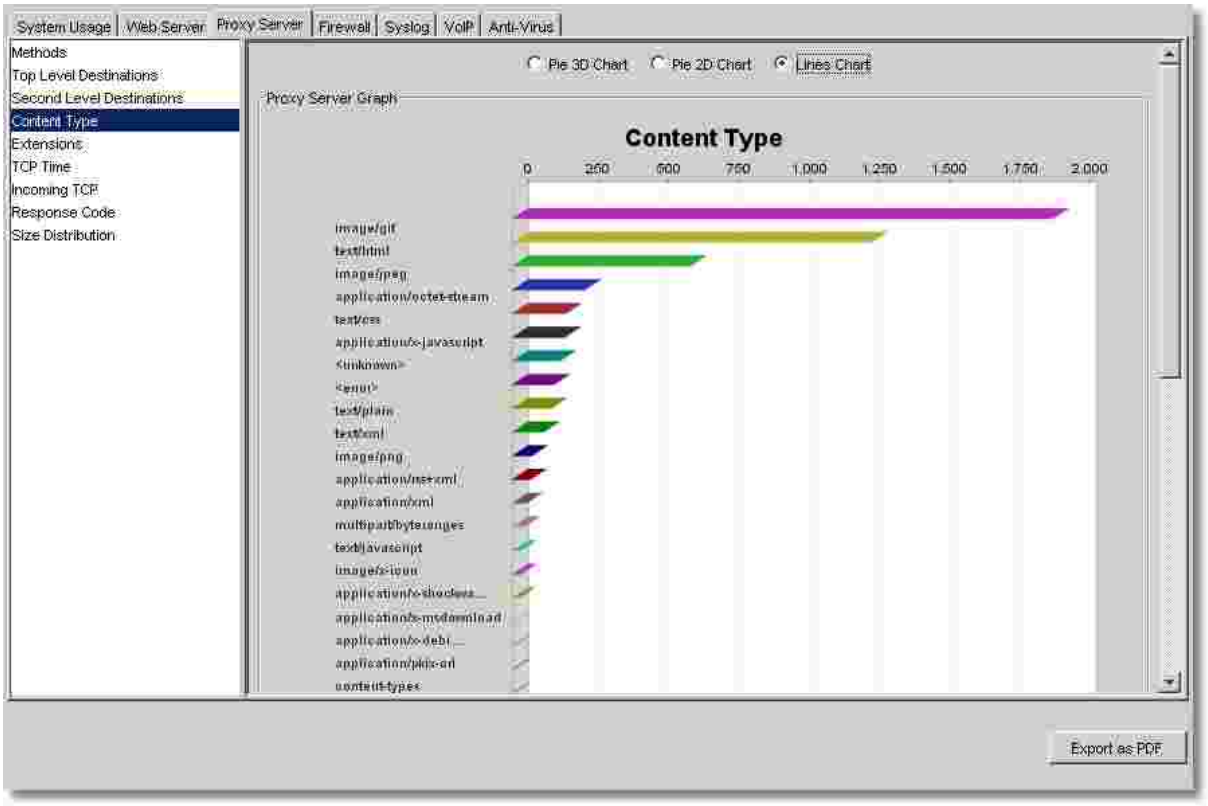
8.3.4 Content Type

This report shows the type of content of the files passing through the proxy server, for example:

- text/plain
- application/octet-stream
- application/x-msn-messenger
- image/gif

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

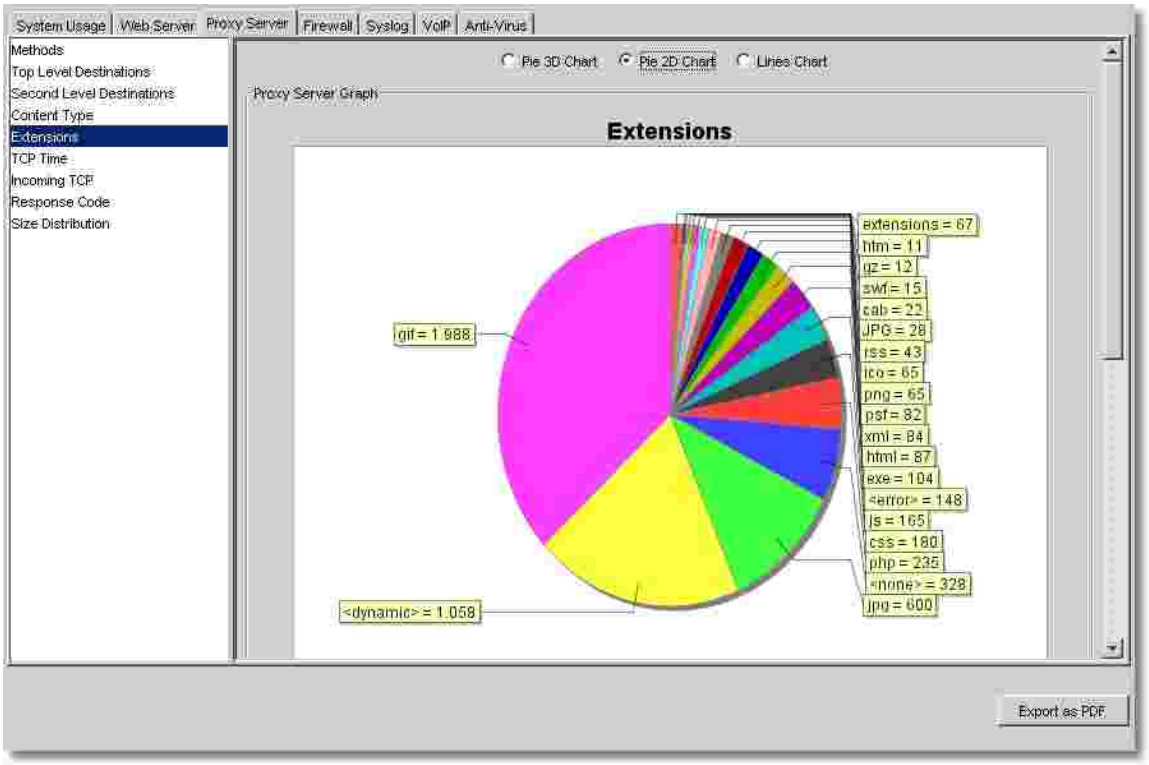
© 2006 Critical Links, SA



8.3.5 Extensions

This report shows the types of extensions for the files passing through the proxy server, for example gif or exe.
This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA



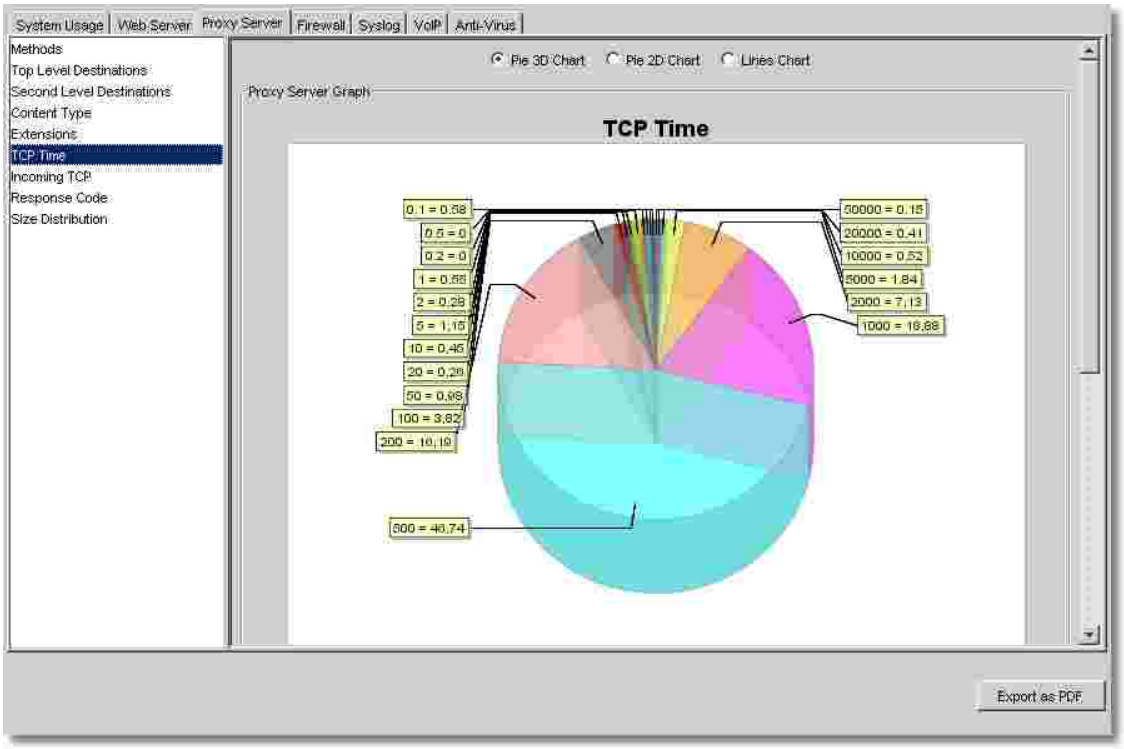
8.3.6 TCP Time

This report shows the values of the TCP time (time the proxy server takes to process a client request) in milliseconds, organised by ranges. The values displayed will be, for example:

- <= 0.1 msec
- <= 0.2 msec
- <= 100000 msec
- <= 1e10 msec

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA



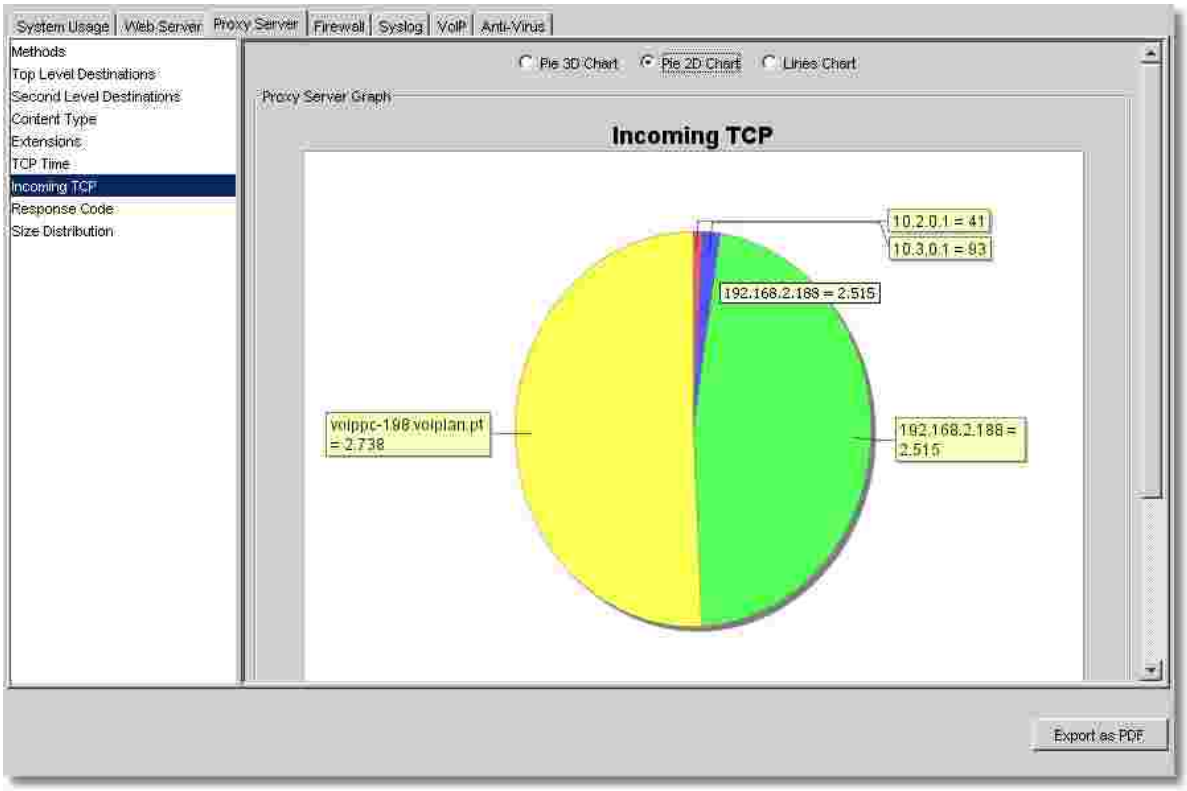
8.3.7 Incoming TCP

This report shows the incoming TCP, i.e. the number of occurrences of IP client requests, presented per IP. The values displayed will be, for example:

- 192.168.3.9
- 192.168.2.4
- 192.168.3.212
- 192.168.2.63
- other: 69 requesting hosts

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

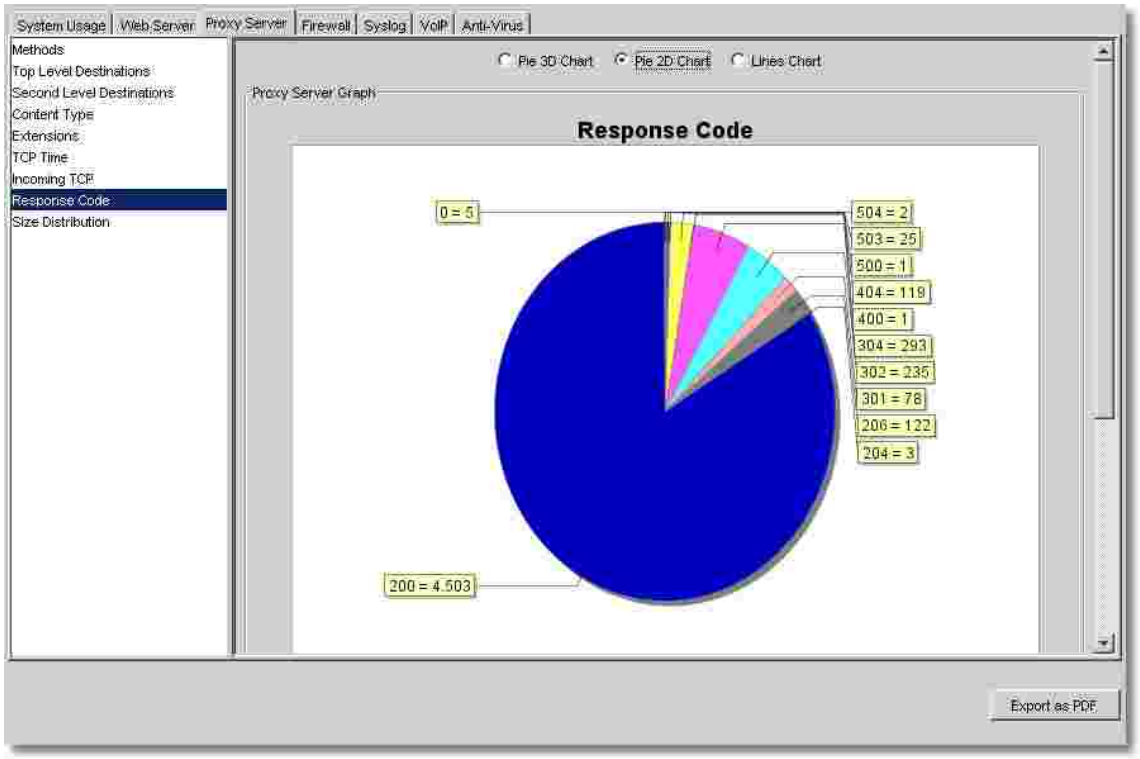


8.3.8 Response Code

This report shows the number of occurrences of the response codes from the proxy server. For a complete list of response codes, please check HTTP status codes.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

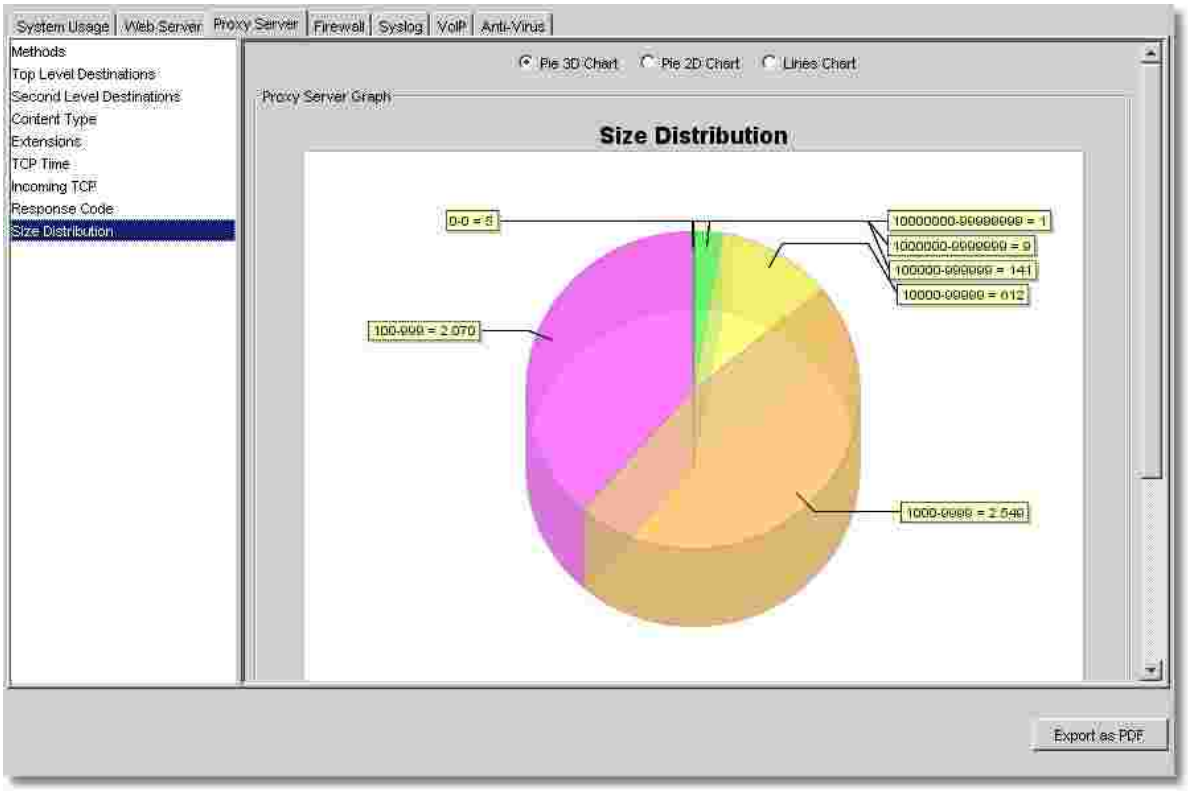


8.3.9 Size Distribution

This report shows the size distribution of the files passing through the proxy server, in bytes, organised by ranges.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA



8.4 Firewall

The reports in this group show information about edgeBOX's firewall. It is possible to export them in pdf format.

8.4.1 Firewall

This report provides general information of the firewall behaviour.

It is possible to customise a filter to limit the data presented and make analysis easier. The following fields are available:

- date (must use the format yyyy-mm-dd);
- type of protocol (All, UDP or TCP);
- interface (All, LAN, WAN or EWAN);
- destination port;
- destination address.

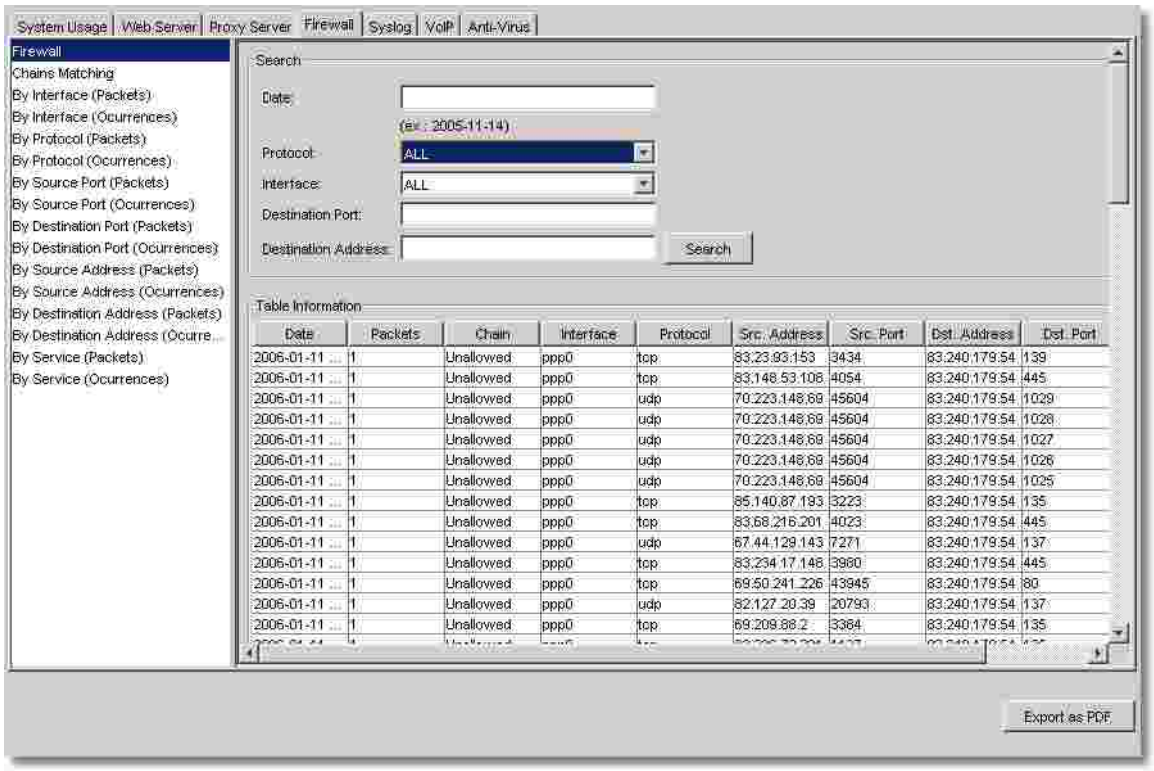
You will have to press the 'Search' button to retrieve the data.

The results of the applied filter are presented in a table with the following columns:

- Date – last 100 entries or selected dates;
- Packets – number of rejected packets;
- Chain – reason why the packet was rejected (for example, dangerous, un-allowed, …)
- Interface – physical interface where the rejected packet arrived (for example, eth0, …)

© 2006 Critical Links, SA

- Protocol – protocol used in the rejected packet (TCP, UDP or ICMP)
- Src. Adress – source address of the rejected packet
- Src. Port – source port of the rejected packet
- Dst. Address - destination address (IP the packet was trying to access)
- Dst. Port – destination port (specific port the packet was trying to access)
- Service – type of service of the packet, if applicable (for example, HTTP, HTTPS, FTP…)

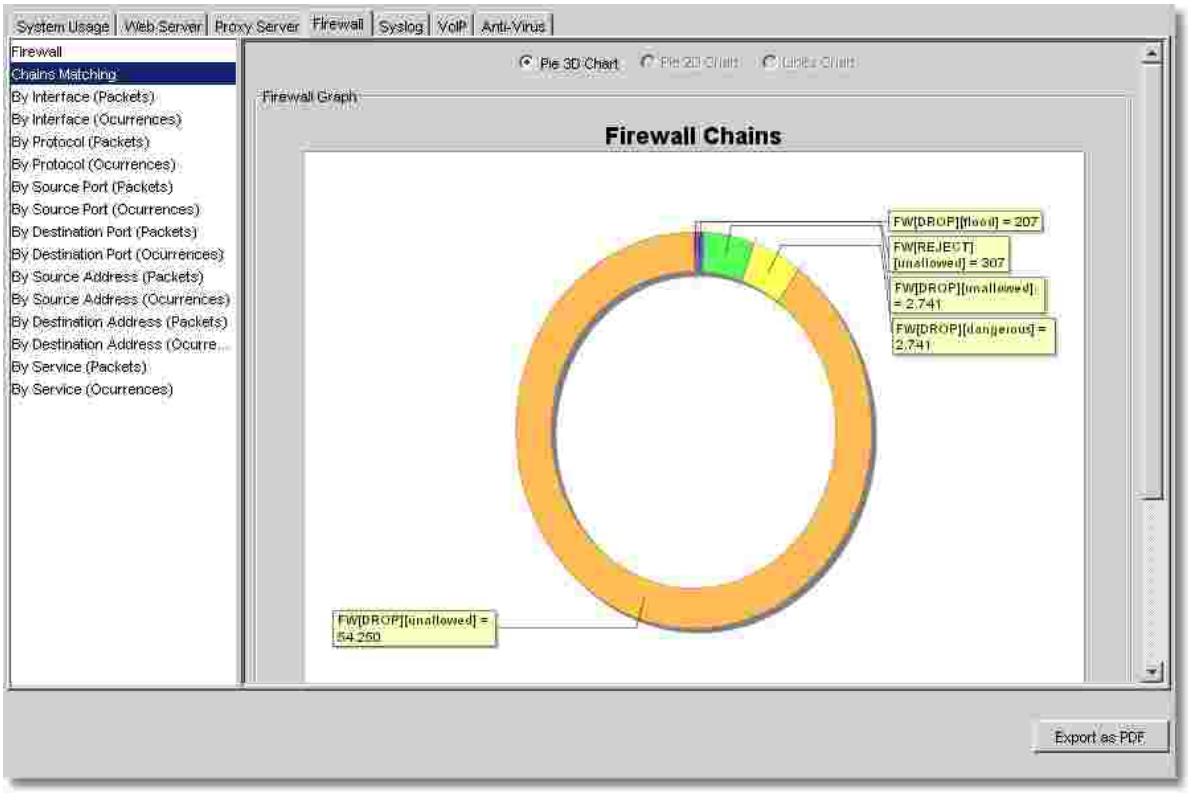

System Usage
Web Server
Proxy Server
Firewall
Syslog
VoIP
Anti-Virus
Firewall
Chains Matching
By Interface (Packets)
By Interface (Ocurrences)
By Protocol (Packets)
By Protocol (Ocurrences)
By Source Port (Packets)
By Source Port (Ocurrences)
By Destination Port (Packets)
By Destination Port (Ocurrences)
By Source Address (Packets)
By Source Address (Ocurrences)
By Destination Address (Packets)
By Destination Address (Ocurre...
By Service (Packets)
By Service (Ocurrences)
Search
Date:
(ex : 2005-11-14)
Protocol:
ALL
Interface:
ALL
Destination Port:
Destination Address:
Search
Table Information
Date
Packets
Chain
Interface
Protocol
Src. Address
Src. Port
Dst. Address
Dst. Port
2006-01-11 ... 1 Unallowed ppp0 tcp 83.23.93.153 3434 83.240.179.54 139
2006-01-11 ... 1 Unallowed ppp0 tcp 83.148.53.108 4054 83.240.179.54 445
2006-01-11 ... 1 Unallowed ppp0 udp 70.223.148.69 45604 83.240.179.54 1029
2006-01-11 ... 1 Unallowed ppp0 udp 70.223.148.69 45604 83.240.179.54 1028
2006-01-11 ... 1 Unallowed ppp0 udp 70.223.148.69 45604 83.240.179.54 1027
2006-01-11 ... 1 Unallowed ppp0 udp 70.223.148.69 45604 83.240.179.54 1026
2006-01-11 ... 1 Unallowed ppp0 udp 70.223.148.69 45604 83.240.179.54 1025
2006-01-11 ... 1 Unallowed ppp0 tcp 85.140.87.193 3223 83.240.179.54 135
2006-01-11 ... 1 Unallowed ppp0 tcp 83.58.216.201 4023 83.240.179.54 445
2006-01-11 ... 1 Unallowed ppp0 udp 67.44.129.143 7271 83.240.179.54 137
2006-01-11 ... 1 Unallowed ppp0 tcp 83.234.17.146 3980 83.240.179.54 445
2006-01-11 ... 1 Unallowed ppp0 tcp 69.50.241.226 43945 83.240.179.54 80
2006-01-11 ... 1 Unallowed ppp0 udp 82.127.20.39 20793 83.240.179.54 137
2006-01-11 ... 1 Unallowed ppp0 tcp 69.209.88.2 3384 83.240.179.54 135
Export as PDF

8.4.2 Chains Matching

This report shows the number of occurrences of the types of chain matching (reason why package was rejected), for example, dangerous, un-allowed.

This information is presented in graphical (Pie 3D) and tabular format.

© 2006 Critical Links, SA

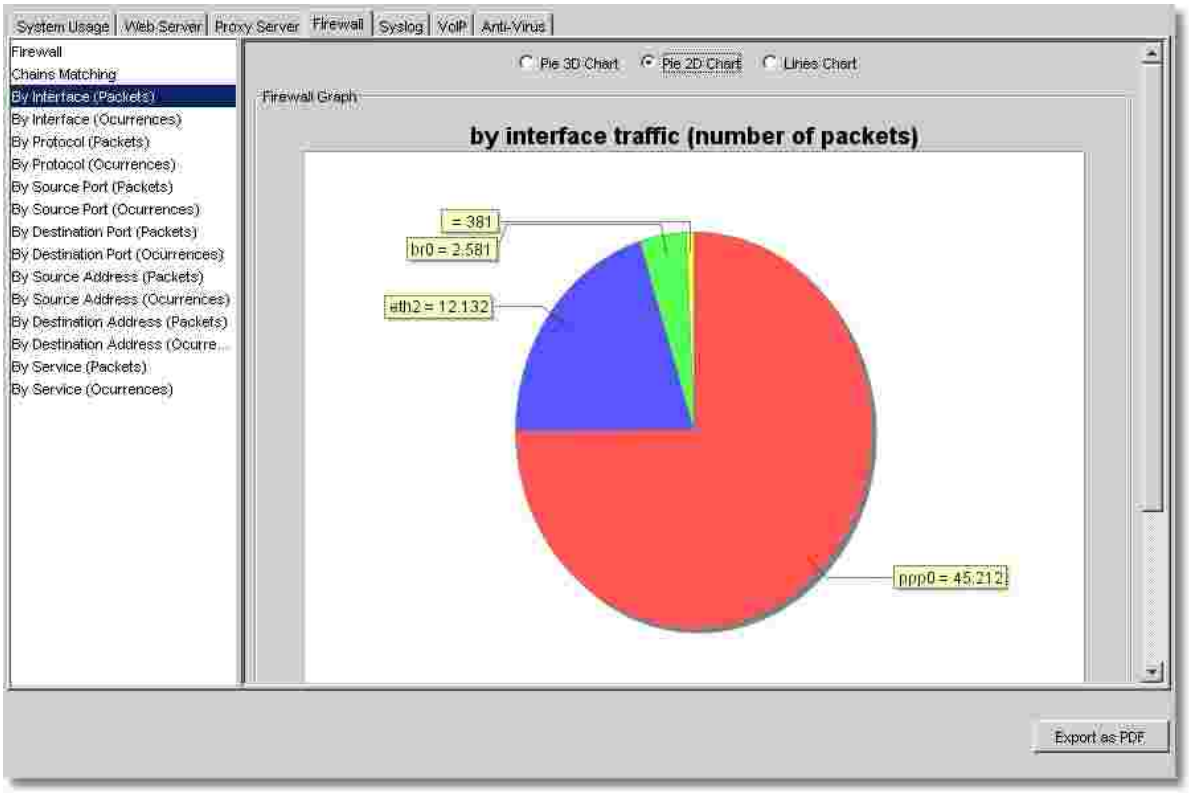


8.4.3 By Interface (Packets)

This report shows the rejected traffic per physical interface (eth0, etc.), in packets.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

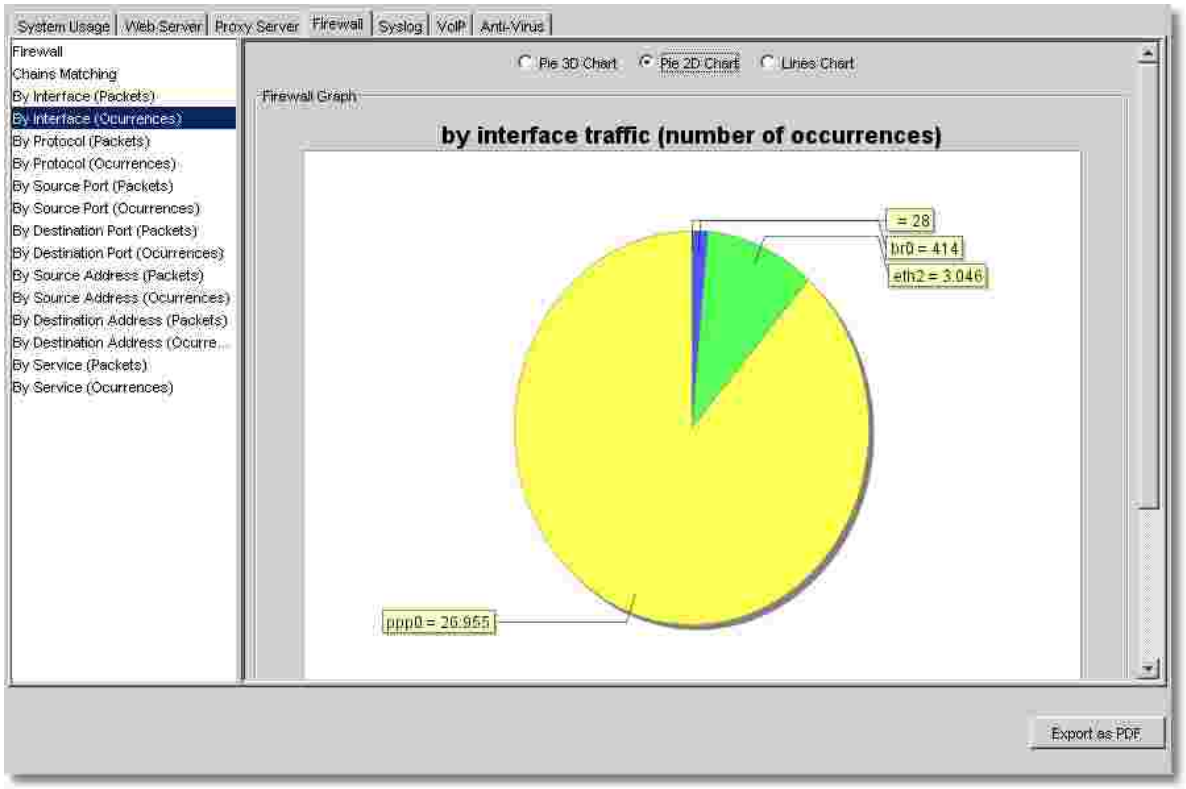


8.4.4 By Interface (Occurrences)

This report shows the number of occurrences traffic was rejected per physical interface (eth0, etc.).

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

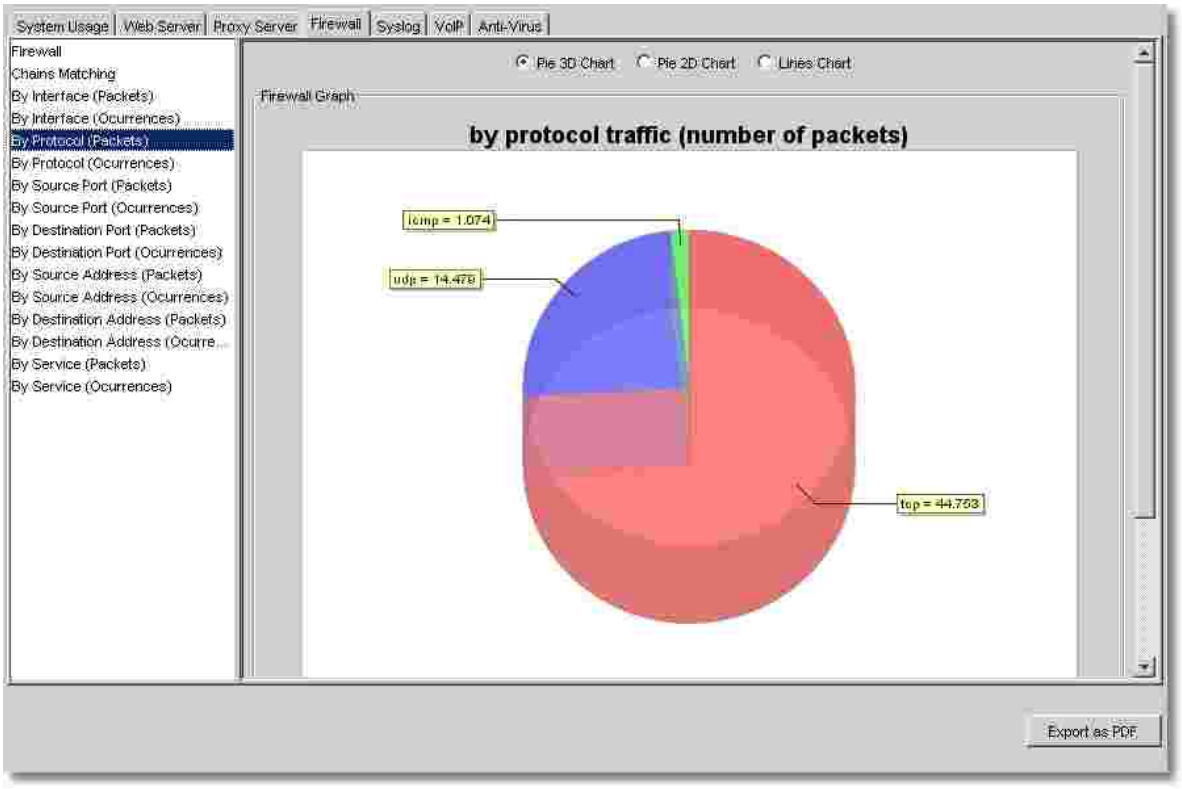


8.4.5 By Protocol (Packets)

This report shows the rejected traffic in all the physical interfaces per protocol (TCP, UDP, etc.), in packets.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

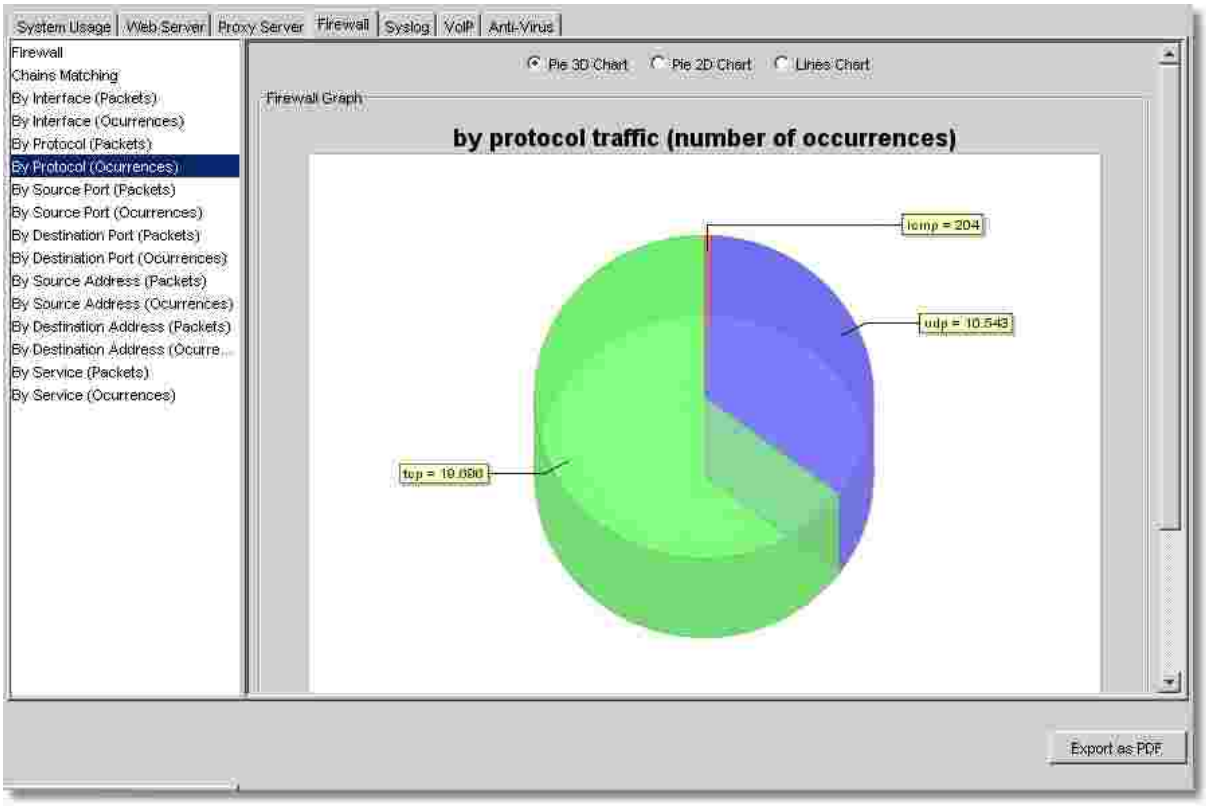


8.4.6 By Protocol (Occurrences)

This report shows the number of occurrences traffic was rejected per protocol (TCP, UDP, etc.).

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

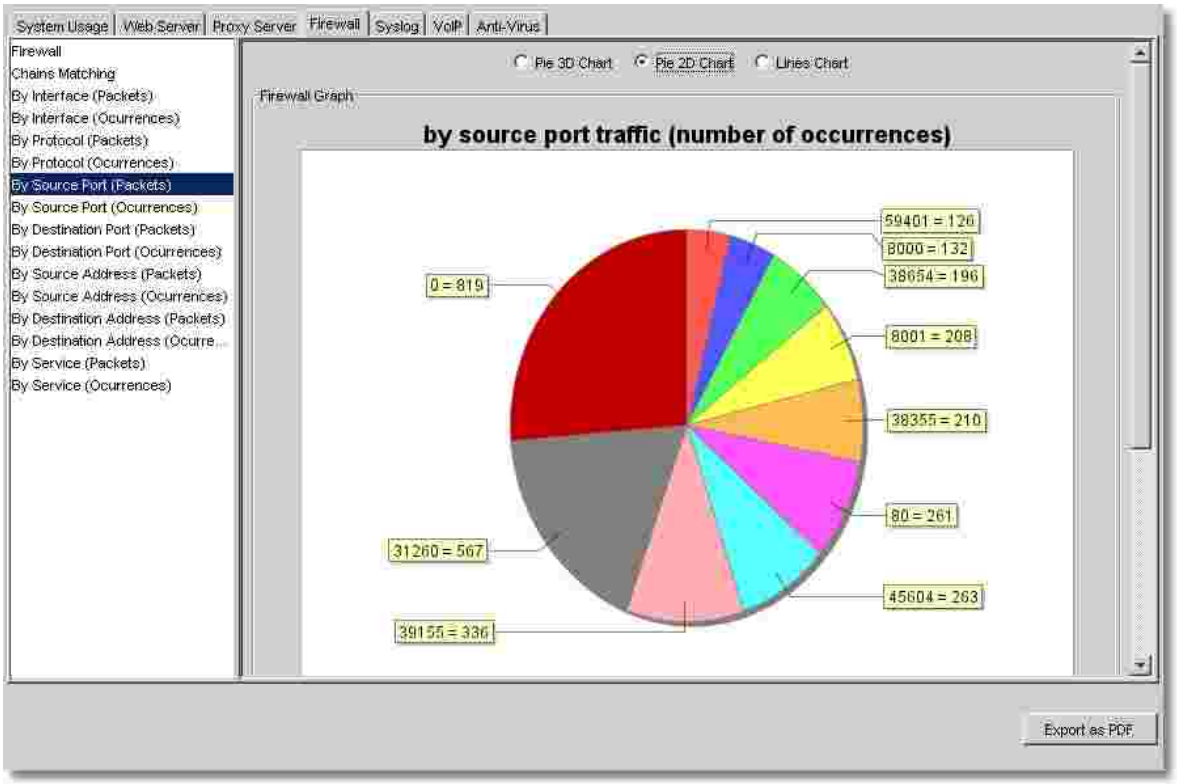


8.4.7 By Source Port (Packets)

This report shows the rejected traffic per source port, in packets.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

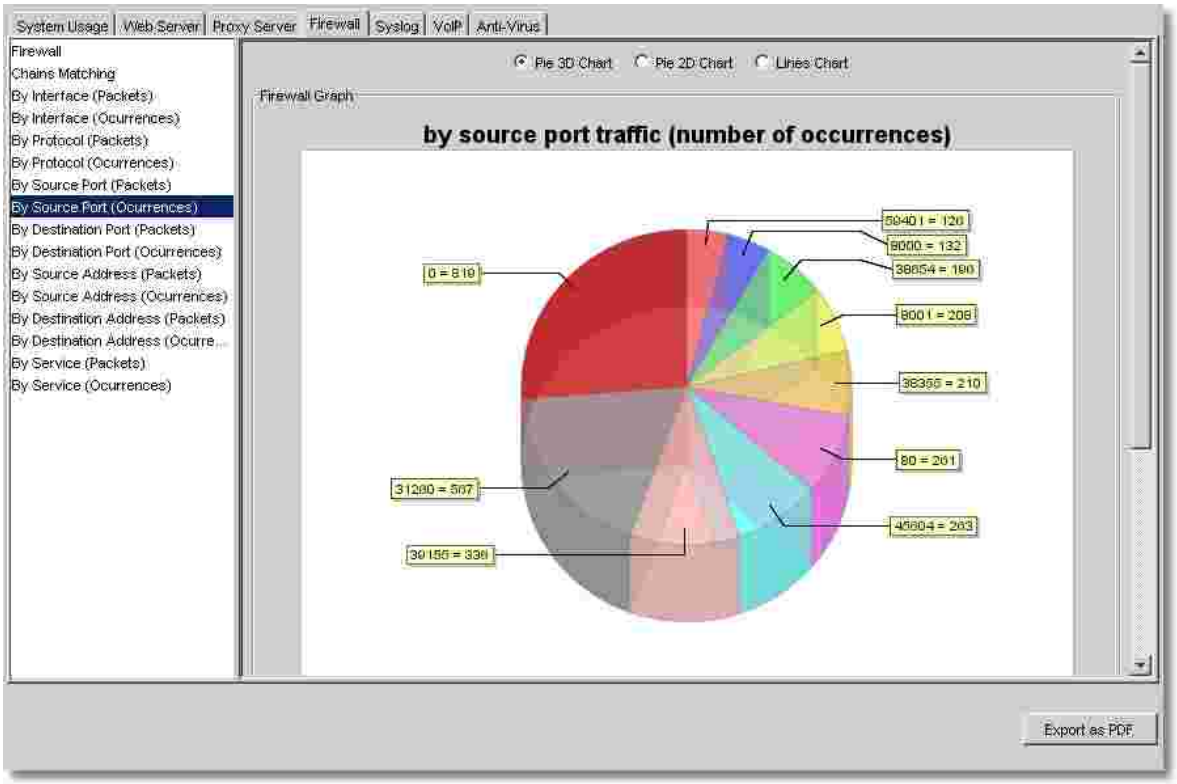


8.4.8 By Source Port (Occurrences)

This report shows the number of occurrences traffic was rejected per source port.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

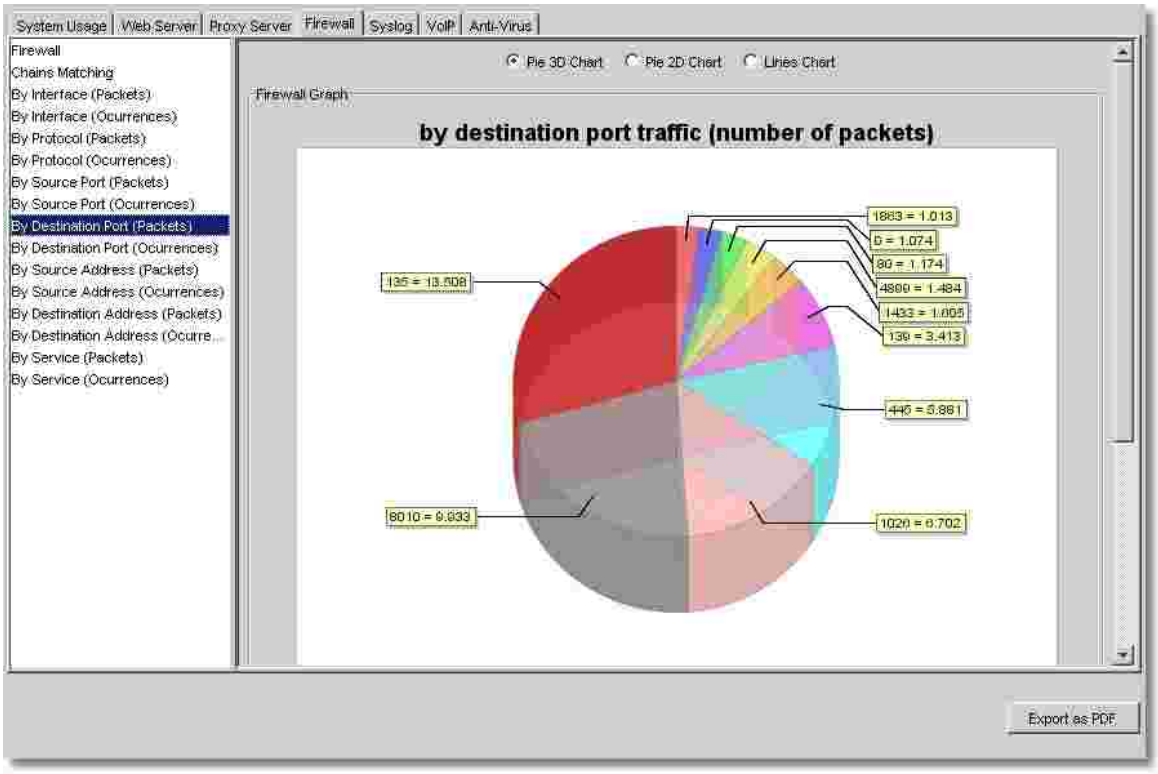


8.4.9 By Destination Port (Packets)

This report shows the rejected traffic per destination port, in packets.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

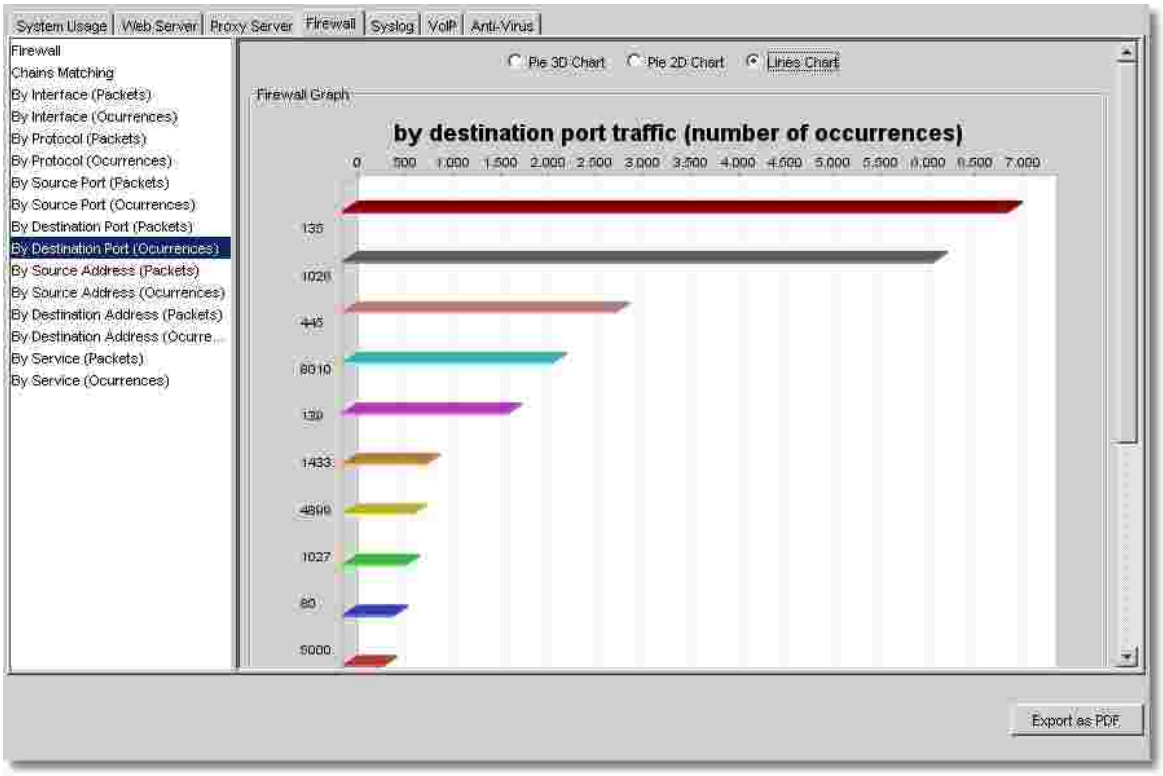


8.4.10 By Destination Port (Occurrences)

This report shows the number of occurrences traffic was rejected per destination port.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

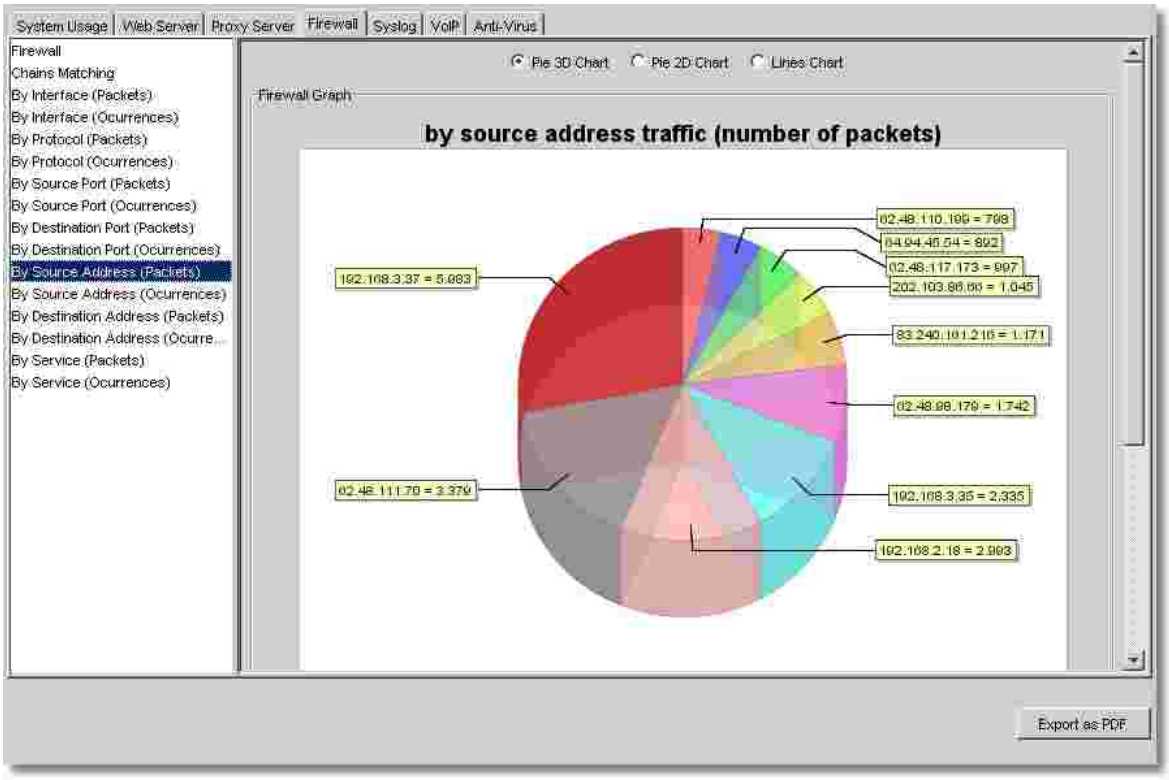


8.4.11 By Source Address (Packets)

This report shows the rejected traffic per source address, in packets.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

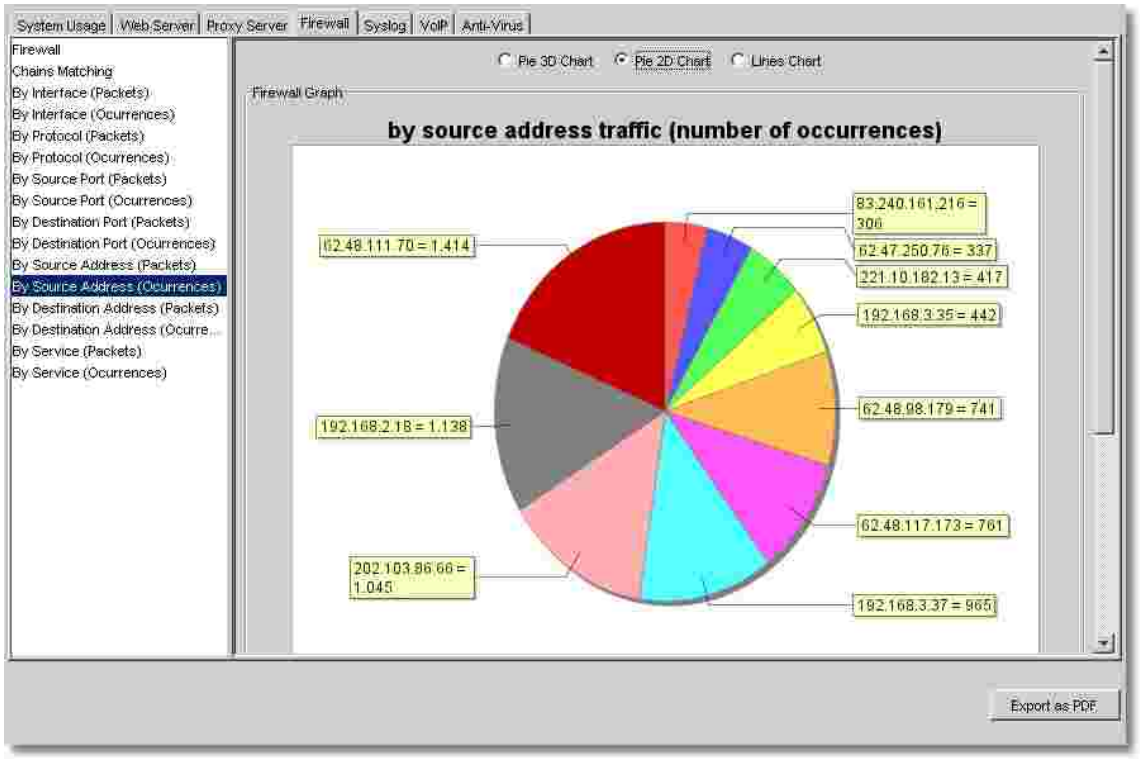


8.4.12 By Source Address (Occurrences)

This report shows the number of occurrences traffic was rejected per source address.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

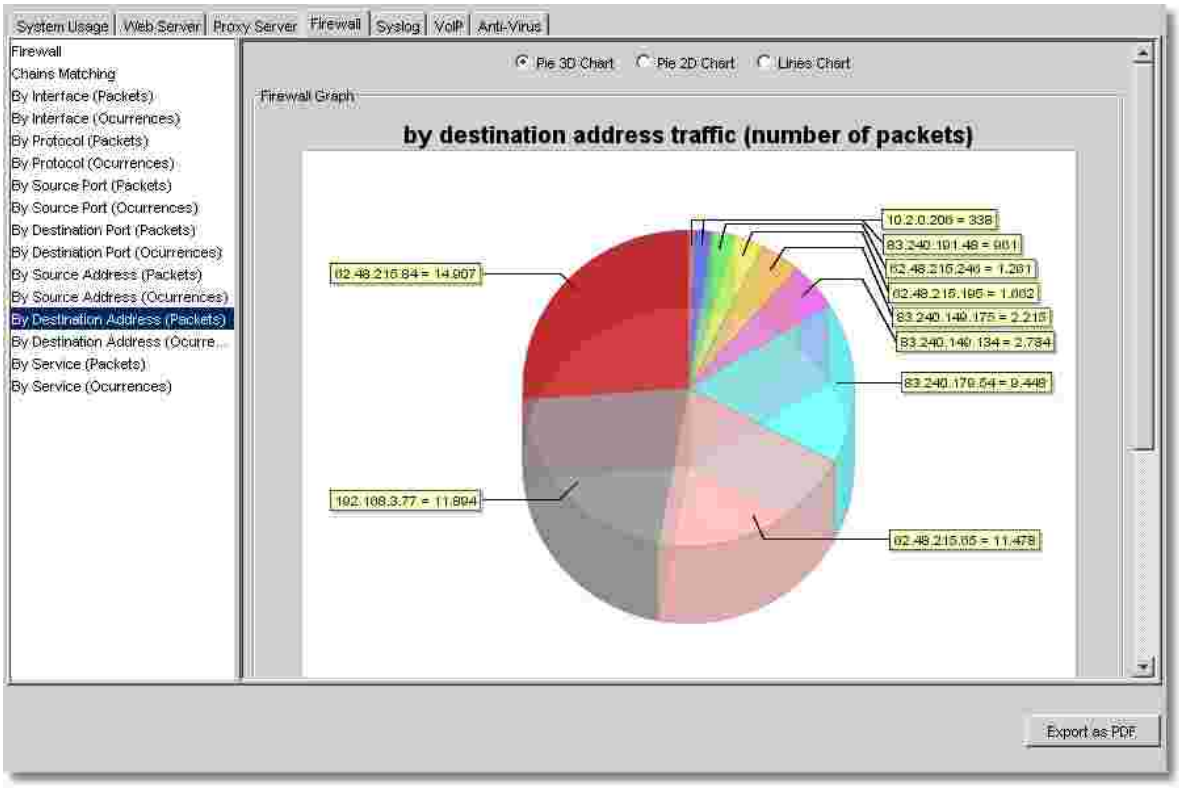


8.4.13 By Destination Address (Packets)

This report shows the rejected traffic per destination address, in packets.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

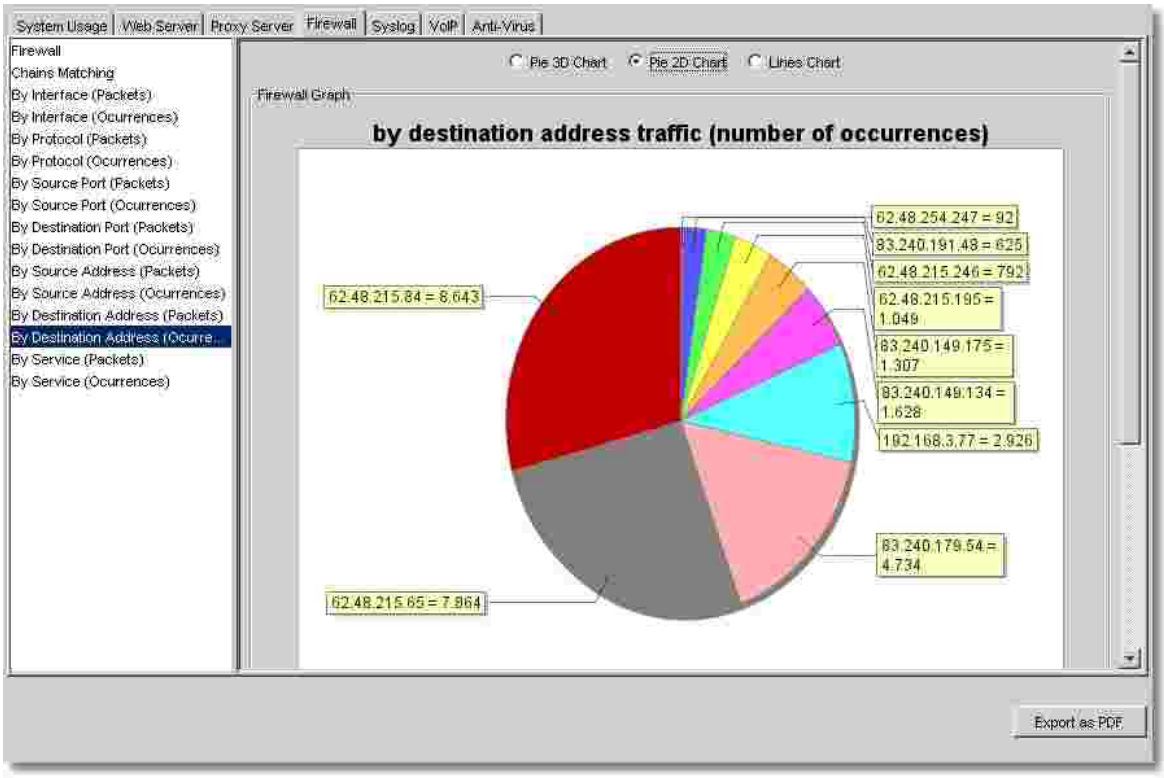


8.4.14 By Destination Address (Occurrences)

This report shows the number of occurrences traffic was rejected per destination address.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

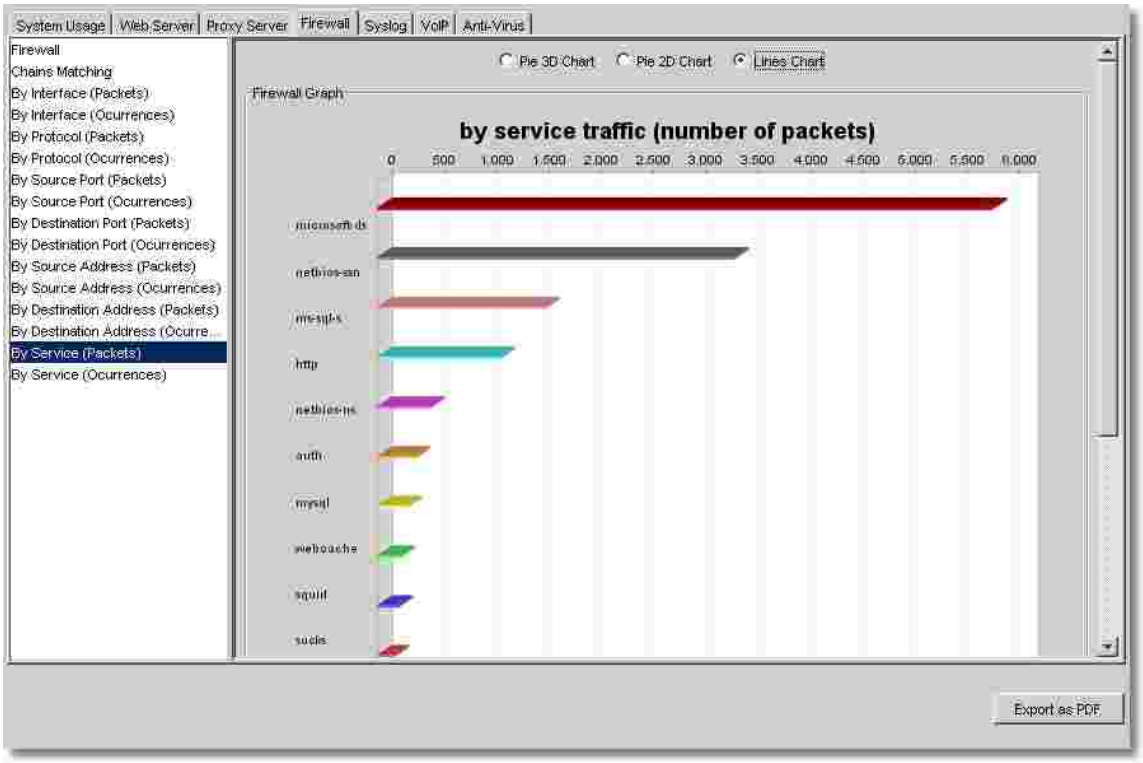


8.4.15 By Service (Packets)

This report shows the rejected traffic per service (e.g. http), in packets.

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA

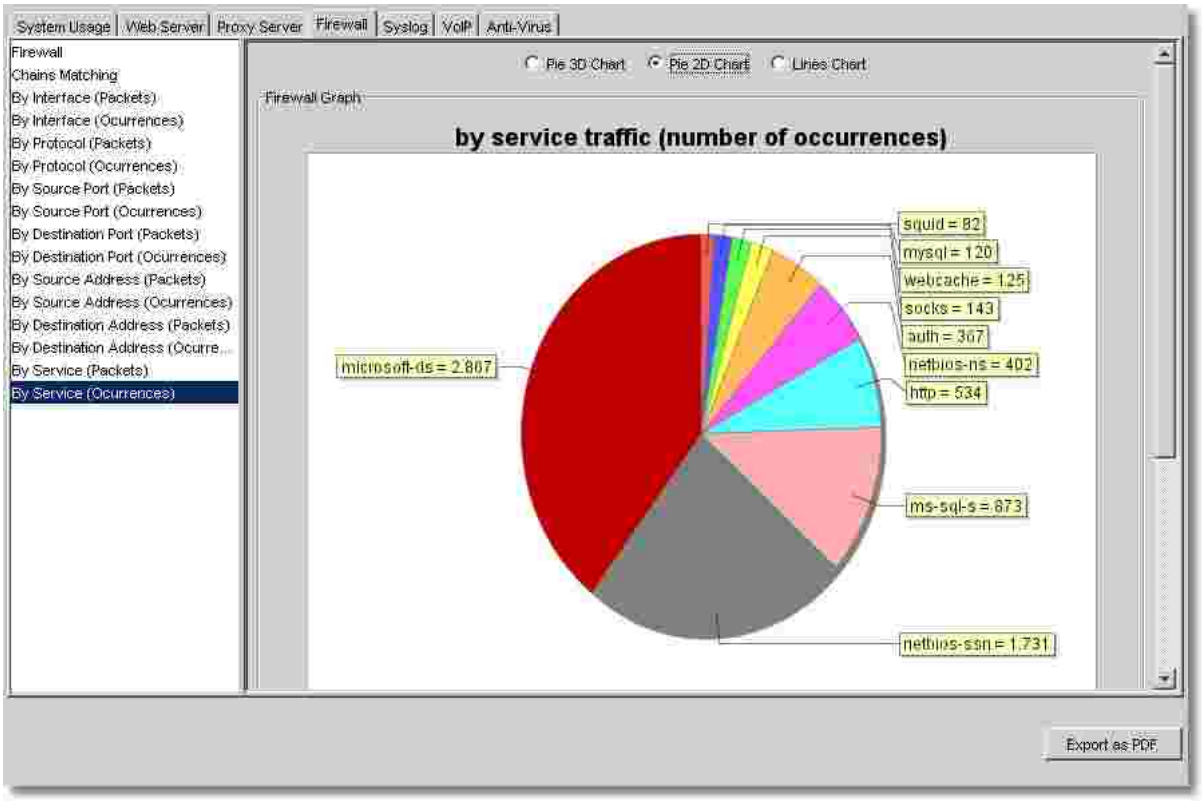


8.4.16 By Service (Occurrences)

This report shows the number of occurrences traffic was rejected per service (e.g. http).

This information is presented in graphical (Pie 3D, Pie 2D or line, selected by clicking the radio button) and tabular format.

© 2006 Critical Links, SA



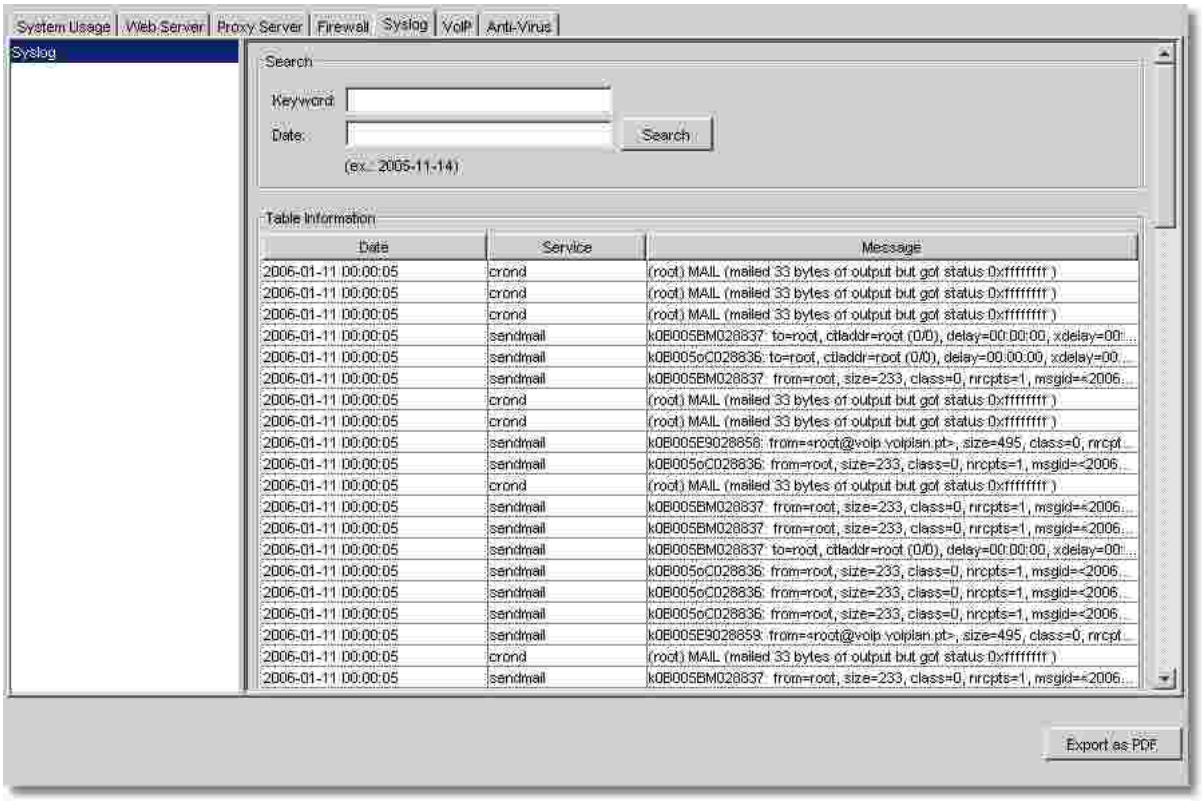
8.5 Syslog

This report shows information about system logs. It can be exported in pdf format.

It is possible to customise a filter – fill keyword - to limit the data presented and make analysis easier. You will have to press the 'Search' button to retrieve the data.

The results will be presented in a table with the date, the service (for example, sendmail) and the message (generated by the respective service).

© 2006 Critical Links, SA


System Usage
Web Server
Proxy Server
Firewall
Syslog
VoIP
Anti-Virus
Syslog
Search
Keyword:
Date:
Search
(ex: 2005-11-14)
Table Information
Date
Service
Message
2006-01-11 00:00:05 crond (root) MAIL (mailed 33 bytes of output but got status 0xffffffff)
2006-01-11 00:00:05 crond (root) MAIL (mailed 33 bytes of output but got status 0xffffffff)
2006-01-11 00:00:05 crond (root) MAIL (mailed 33 bytes of output but got status 0xffffffff)
2006-01-11 00:00:05 sendmail k0B005BM028837: to=root, ctladdr=root (0/0), delay=00:00:00, xdelay=00:...
2006-01-11 00:00:05 sendmail k0B005oC028836: to=root, ctladdr=root (0/0), delay=00:00:00, xdelay=00:...
2006-01-11 00:00:05 sendmail k0B005BM028837: from=root, size=233, class=0, nrcpts=1, msgid=<2006...
2006-01-11 00:00:05 crond (root) MAIL (mailed 33 bytes of output but got status 0xffffffff)
2006-01-11 00:00:05 crond (root) MAIL (mailed 33 bytes of output but got status 0xffffffff)
2006-01-11 00:00:05 sendmail k0B005E9028858: from=<root@voip.voipian.pt>, size=495, class=0, nrcpt...
2006-01-11 00:00:05 sendmail k0B005oC028836: from=root, size=233, class=0, nrcpts=1, msgid=<2006...
2006-01-11 00:00:05 crond (root) MAIL (mailed 33 bytes of output but got status 0xffffffff)
2006-01-11 00:00:05 sendmail k0B005BM028837: from=root, size=233, class=0, nrcpts=1, msgid=<2006...
2006-01-11 00:00:05 sendmail k0B005BM028837: from=root, size=233, class=0, nrcpts=1, msgid=<2006...
2006-01-11 00:00:05 sendmail k0B005BM028837: to=root, ctladdr=root (0/0), delay=00:00:00, xdelay=00:...
2006-01-11 00:00:05 sendmail k0B005oC028836: from=root, size=233, class=0, nrcpts=1, msgid=<2006...
2006-01-11 00:00:05 sendmail k0B005oC028836: from=root, size=233, class=0, nrcpts=1, msgid=<2006...
2006-01-11 00:00:05 sendmail k0B005oC028836: from=root, size=233, class=0, nrcpts=1, msgid=<2006...
2006-01-11 00:00:05 sendmail k0B005E9028859: from=<root@voip.voipian.pt>, size=495, class=0, nrcpt...
2006-01-11 00:00:05 crond (root) MAIL (mailed 33 bytes of output but got status 0xffffffff)
2006-01-11 00:00:05 sendmail k0B005BM028837: from=root, size=233, class=0, nrcpts=1, msgid=<2006...
Export as PDF

8.6 VoIP

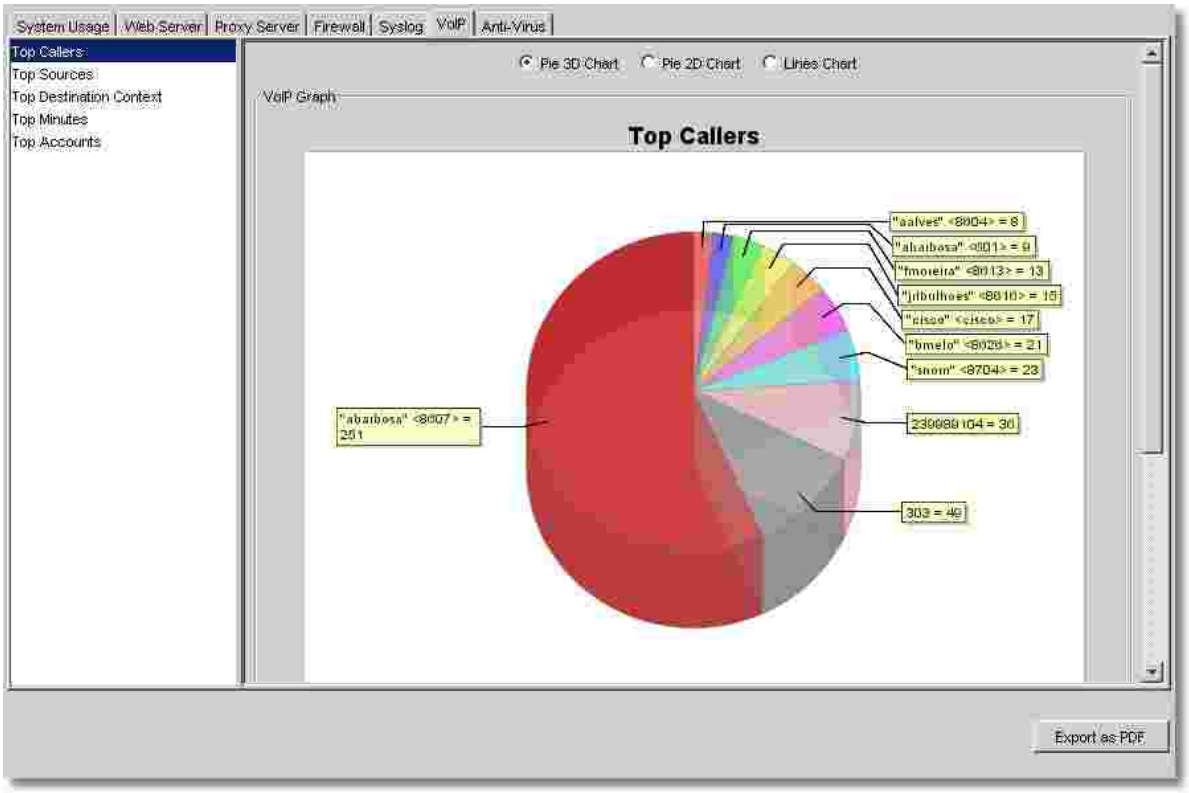
The reports in this group show information about edgeBOX's VoIP functionality and are presented in both graphical and tabular format. It is possible to export them in pdf format.

8.6.1 Top Callers

This report shows the top 10 number of calls per caller id (phone where the call originated).

The values presented in this report will be very similar to the ones in Top Sources (unless there is an extension or phone change).

© 2006 Critical Links, SA

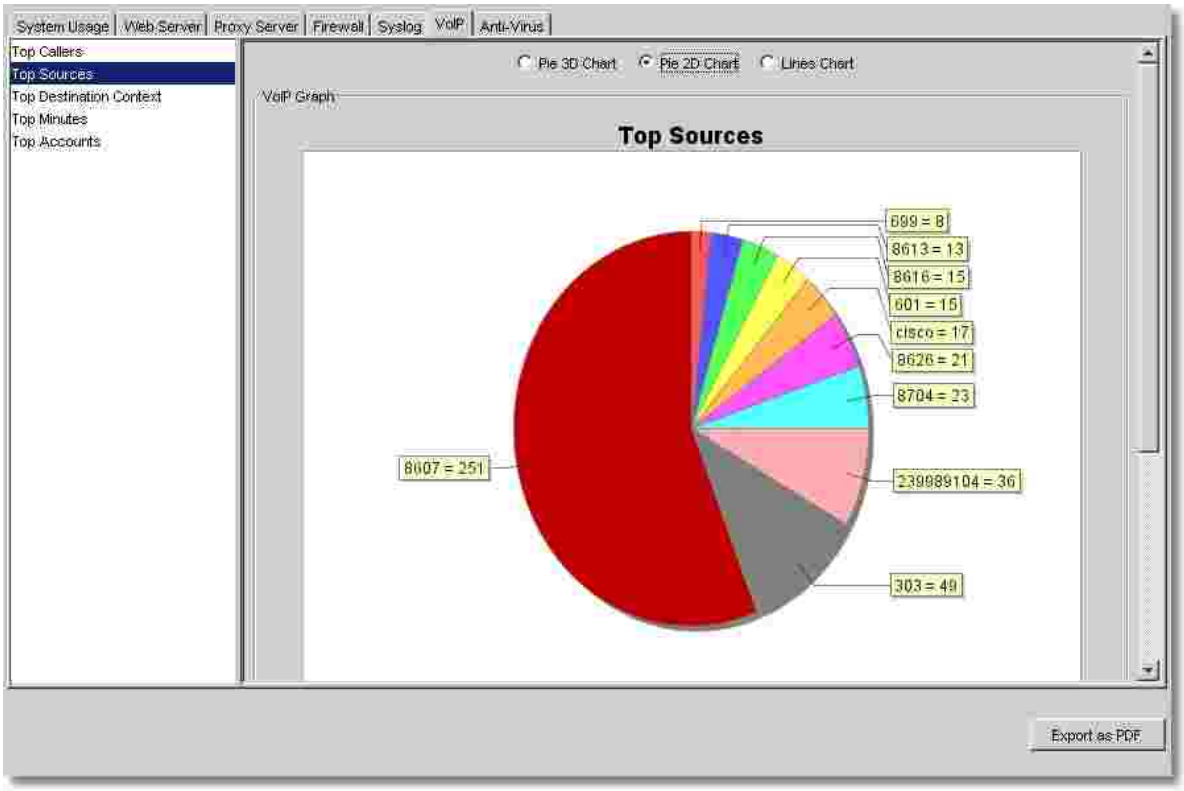


8.6.2 Top Sources

This report shows the top 10 number of calls per source (extension where the call originated, for example 8601).

The values presented in this report will be very similar to the ones in Top Callers (unless there is an extension or phone change).

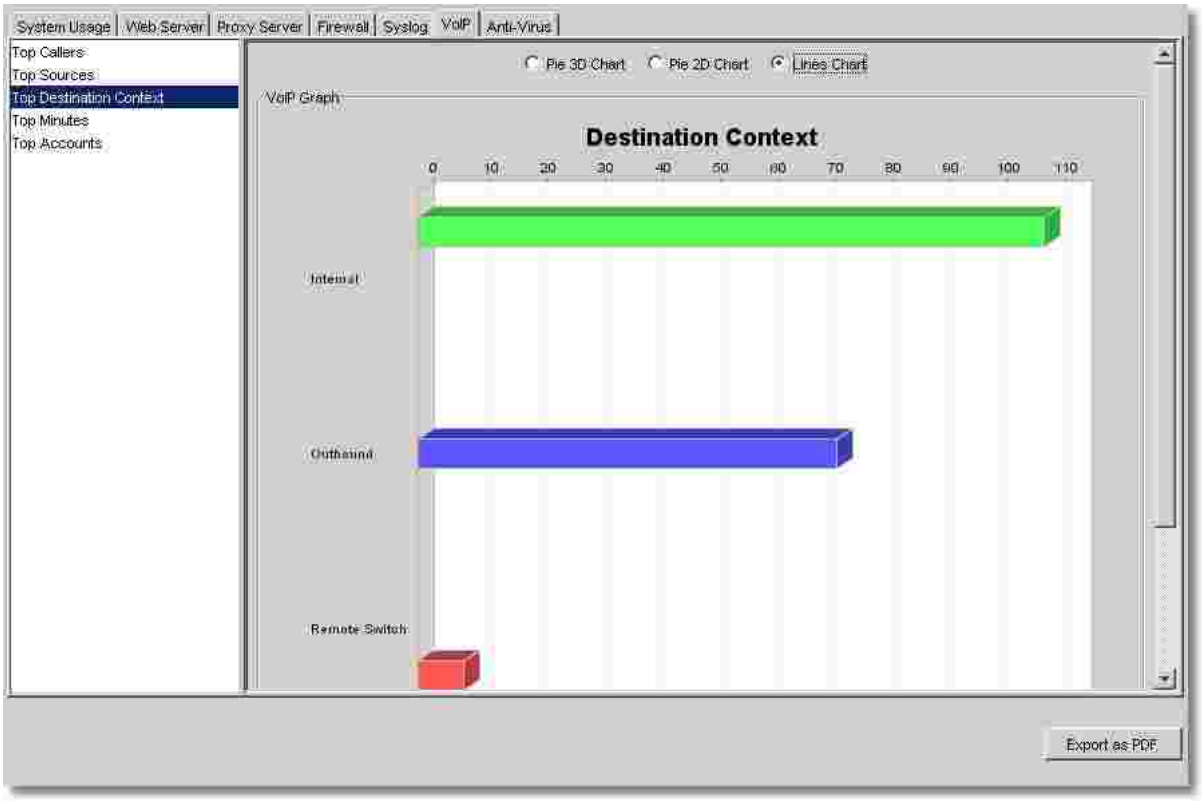
© 2006 Critical Links, SA



8.6.3 Top Destination Context

This report shows the top 10 number of calls per destination context, i.e. internals (calls to the same edgeBOX), remote (calls to a different edgeBOX) and outbound (external calls, to PSTN or PLMN).

© 2006 Critical Links, SA



8.6.4 Top Minutes

This report shows the top 10 number of calls per caller id (phone where the call originated), in minutes.

This report will only present results if authentication is on.

8.6.5 Top Accounts

This report shows the top 10 number of calls per account (pin, corresponding to a specific user or group of users) that initiated a call.

This report will only present results if authentication is on.

8.7 Anti-Virus

The reports in this group show information about edgeBOX's anti virus. It is possible to export them in pdf format.

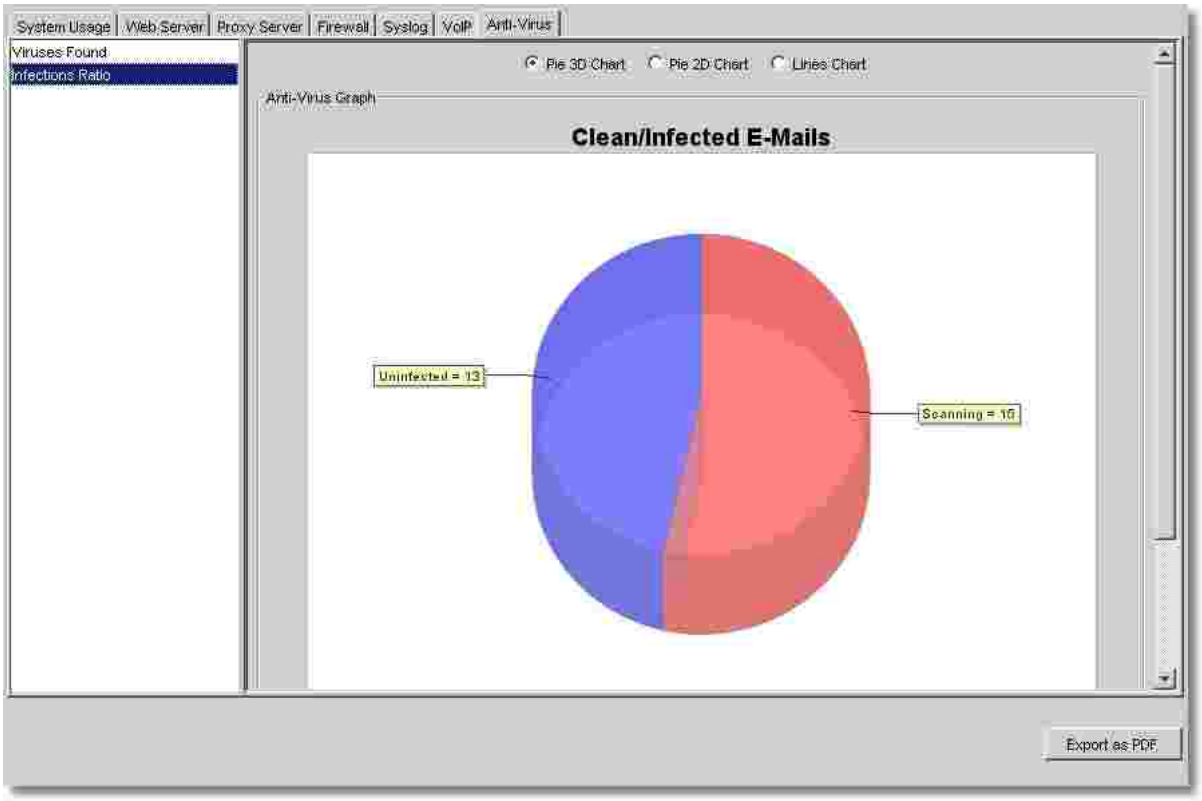
8.7.1 Viruses Found

This report shows the top 10 viruses found in e-mail passing through the box.

8.7.2 Infections Ratio

This report shows the ratio of e-mails passing through the box clean Vs infected.

© 2006 Critical Links, SA



© 2006 Critical Links, SA

9 Appendix A: Authentication

edgeBOX runs several services under which you have to provide credentials. There are a whole lot of possible authentication scenarios and configurations. In this appendix, edgeBOX's authentication architecture will be explained. It is important to understand these concepts, as they will be needed if you want to deploy a remote authentication scenario. Next, it will be shown what happens when the "Require users to login" option is enabled. Finally, the complete sequence of events will be reviewed and detailed. Finally, some remote configuration examples will be shown.

9.1 Authentication architecture

Authentication (proving who you are) and authorisation (what you can do) are handled in a mixed manner in edgeBOX. Considering first a local authentication scenario, upon user creation you need to provide a password and define which services a user will be authorised to use. Services available in edgeBOX are:

- Regular services, such as POP3, IMAP, FTP and Internet access for LAN users;
- Windows use (Samba);
- Wireless 802.1x;
- PPTP and
- VoIP.

Internally, edgeBOX uses a Radius server configured to use a LDAP backend.

9.2 Require users to login vs Group Policies

Connections originating from the LAN to the Internet, to the Enterprise network and to services running on edgeBOX are granted by default. But you may choose to limit this access by enforcing an access policy. This is done by enabling "Require users to login" on the Firewall panel. The policies are enforced at the firewall level.

This is always the first level of access to be tested - if users are required to login (here 'users' refer to LAN users), any connections of the type mentioned above (the exceptions is to edgeBOX's authentication page and to edgeBOX's control centre) are denied - they are in fact discarded by the firewall.

If an user wants to access the Internet, the following steps must be taken:

- The user accesses edgeBOX's authentication page or some website running on port 80 (which causes a redirection to edgeBOX's authentication page);
- The user enters his credentials (username/password);
- If the credentials entered were valid, the user may or may not be granted access, depending on his group policy.

From this moment on, and if this user's policy grants him access to the Internet, he will be able to access any remote service. Furthermore, a pop-up window will be displayed, allowing him to log out. This pop-up window must be kept open to keep the user authenticated. If this window is closed and no network traffic is detected originating from this user's machine, the authentication will time out and the user will have to re-authenticate in order to access the Internet. The timeout is set to five minutes.

Group policies allow the following items to be configured:

© 2006 Critical Links, SA

- QoS classes assigned to WAN/EWAN connections;
- Access to the Internet: time interval and services;
- Access to edgeBOX's services: time interval and services;
- Access to the EWAN: time interval and services;
- Access to IPsec VPNs.

As have been mentioned before, this kind of policies are handled at the firewall level. After an user authenticates appropriate firewall rules are loaded in order to enforce his group policy. An user authenticating from a PC in the LAN will in fact revert to an IP/MAC address pair, and each rule loaded will refer to this pair. If the group to which the user belongs to was granted access to the Internet, a firewall rule will be loaded allowing all traffic originating from this host to the Internet.

If a group contains an IP address and users are required to login is enabled then firewall rules reflecting this group's policy featuring this IP will automatically be loaded, making it a static entry. A typical use of this feature is to automatically allow servers to access the Internet. Suppose you have a Windows update server. By making its IP a member of a group with access to the Internet will automatically enable access to the Internet for this server.

9.3 Putting all together

Suppose a user inside a LAN tries to access the Internet or an edgeBOX service and "Require users to login" is enabled. The complete sequence of events is as follows:

- If the user tries to access edgeBOX's port 8010, access is granted;
- Otherwise, if the user tries to access a website on port 80 or edgeBOX's authentication page, the authentication page is displayed;
- Otherwise (any other application), access is denied by the firewall.
- After entering his credentials, edgeBOX's Radius server is queried. If a reject argument is found, access is denied (authorisation failed);
- Otherwise, LDAP is queried. if the password does not match, access is denied (authentication failed);
- Otherwise, access is granted (authorisation AND authentication succeeded);
- At this point, rules reflecting this user's group policy are loaded into the firewall. The IP/MAC address pair in these rules are the user's PC IP/MAC address pair.
- If the user has requested a web page and his policy allows, his browser will be redirected to the web page requested and a small window will pop-up, containing a message indicating success and a logout button. Otherwise, access will be denied.
- If the user closes the pop-up window and no network traffic is generated for 5 minutes, the rules will be unloaded from the firewall and further connections denied. The user will have to reauthenticate.
- Otherwise, the user will be granted access according to his policy.

9.4 Remote configuration

So far we have assumed edgeBOX handles both authentication and authorisation using its local radius and ldap servers. However, these two functions can be delegated on remote servers, allowing for a multitude of different configurations and scenarios.

© 2006 Critical Links, SA

Due to the concept of system-wide authentication, all services will be authenticated against the scheme chosen, be it local or remote. There are some services however, namely PPTP and Wireless that allow you to use another (Radius) server to perform authentication.

The following matrix displays the possible combinations for authentication/authorisation schemes.

Authorisation	Authentication
Local Radius	Local LDAP
Local Radius	Remote LDAP
Local Radius	Remote AD
Local Radius	Remote Radius
Remote Radius	Remote Radius
Remote LDAP	Remote LDAP

The first line matches edgeBOX's local configuration (all local). You can have a remote configuration replicating this configuration, in which Radius performs authorisation, having a LDAP backend performing authentication/authorisation.

Special remarks have to be made when you delegate authorisation/authentication on a remote server. As users are remote, they are not known to edgeBOX before they make their first successful login. Before this happens no user account is created locally and the same applies for edgeBOX's local Radius and LDAP servers (edgeBOX always keeps a local copy).

If you are using local authorisation, you will still be able to edit user's permissions. In this scenario, after an user logins in for the first time he will be granted permission to only access regular services.

Bear in mind that although a remote scheme is used, you can still add local users before those users make their first login. This can be useful if you want to set their service permissions beforehand (when using local authorisation) or to set the group to which they will belong (by default they are assigned to the generic group).

When using Active Directory as a remote authentication scheme, you have the option to import the users. In such a configuration, local accounts and entries will be created locally.

Depending on the scheme used, the way an user may perform his first login will vary. The next table displays this information.

Remote authentication scheme used	First login
Local, AD (with user import), remote LDAP	any service: FTP, POP3, PPTP, WiFi, LAN user
remote Radius, AD (without user import)	only using LAN user authentication.

© 2006 Critical Links, SA

10 Appendix B: VPN Setup

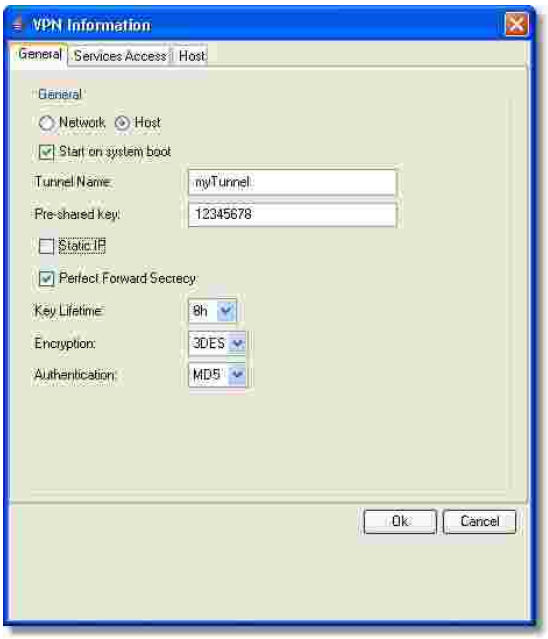
In this appendix, it be will shown how to setup a client to connect to edgeBOX's VPN server. Two types of VPSs will be covered: IPSec and PPTP VPNs.

10.1 IPsec VPNs

The following pictures show the configuration used in edgeBOX in order to establish an IPsec VPN connection between a client machine and edgeBOX. The following elements must be consistent in edgeBOX and in the VPN client used:

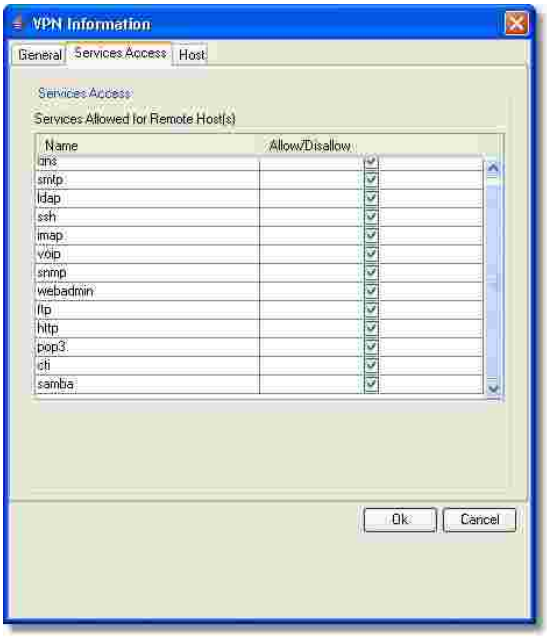
- Pre-shared key: 12345678;
- Encryption: 3DES and
- Authentication: MD5.

Also, IP host configuration will be fetched dinamically (RoadWarrior configuration). The connection must then be initiated by the client.

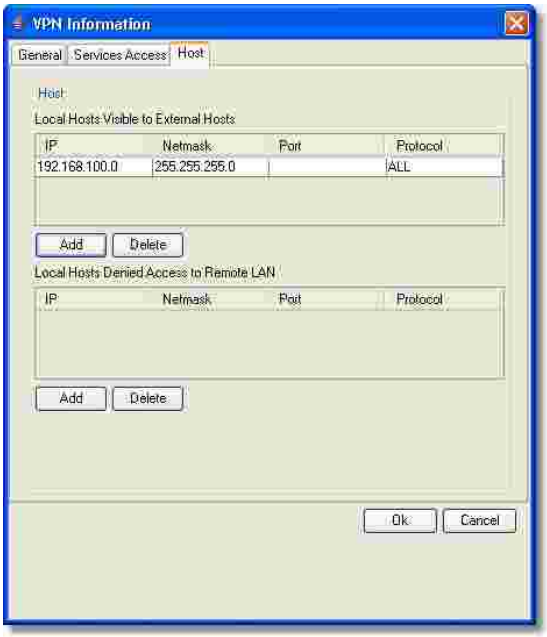


Also, if you wish to be able to access any of edgeBOX's services, then you should check them in the "Services Access" panel:

© 2006 Critical Links, SA



If have to grant access explicitly to the machines you want to access inside edgeBOX's LAN. In the following example, we chose to grant access to all hosts in the internal network.



After applying the data entered, you can start the service. The screen on edgeBOX's control centre will look like the following picture.

© 2006 Critical Links, SA

Next, we will show how to configure and establish a connection using two supported clients: SSH Sentinel and GreenBow.

10.1.1 SSH Sentinel

It will now be shown how to configure an IPsec tunnel using SSH Sentinel. After installing this application, an icon will be visible in the tray bar. After clicking on this icon, a menu will be visible, where the "Run Policy Editor" option should be chosen. On the window that pops up, choose the "Key Management" tab and expand "My Keys". Select "new preshared key" and press the "Add" button. The "New Authentication Key" wizard will be started.

Key management panel

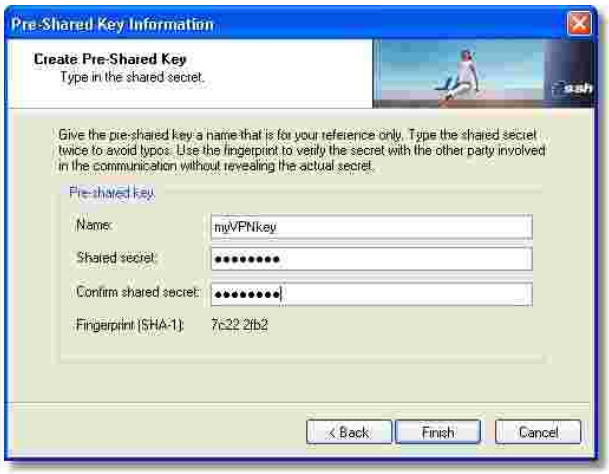
On the initial dialog window, you should choose "Create a pre-shared key", and then select "Next".

© 2006 Critical Links, SA

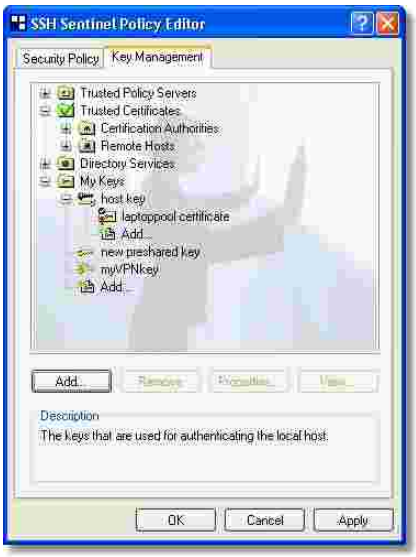
The actual key is entered in the second wizard dialog window, where you should also enter a name to identify this key. After you do this, you may press the "Finish" button.

New Authentication Key
This wizard guides you through the generation of a new authentication key.
What kind of an authentication key would you like to create?
Create an authentication key pair and a certificate
Create a pre-shared key
< Back
Next >
Cancel

initial dialog window


Pre-Shared Key Information
Create Pre-Shared Key
Type in the shared secret.
Give the pre-shared key a name that is for your reference only. Type the shared secret twice to avoid typos. Use the fingerprint to verify the secret with the other party involved in the communication without revealing the actual secret.
Pre-shared key
Name:
myVPNkey
Shared secret:
Confirm shared secret:
Fingerprint (SHA-1):
7c22 2fb2
< Back
Finish
Cancel

entering the pre-shared key



the new key appears under My Keys

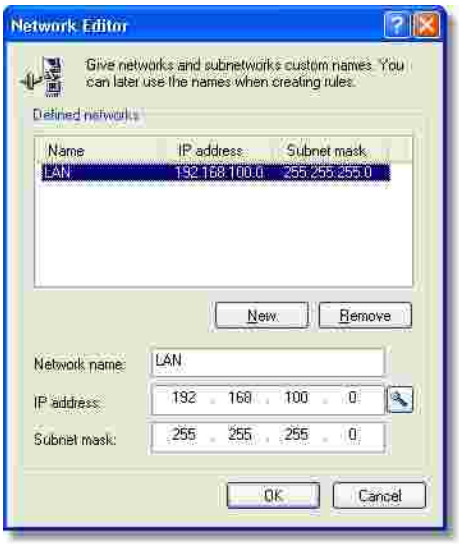
Next, switch to the first tab ("Security Policy"), where the tunnel will be defined. Start by expanding "VPN Connections" and selecting "Add", after which you should press the "Add" button. The "Add VPN Connection" dialog window will pop-up.

© 2006 Critical Links, SA

Security Policy

Add VPN connection

Enter the IP address for the remote gateway in "Gateway name" (in our case it is 192.168.2.180). Select the ... button will make the "Network Editor" window pop-up. In this dialog window you will define the remote network's IP address, as well as its netmask. After pressing "Ok", you will return to the "Add VPN Connection" dialog, where you can choose the network just configured.



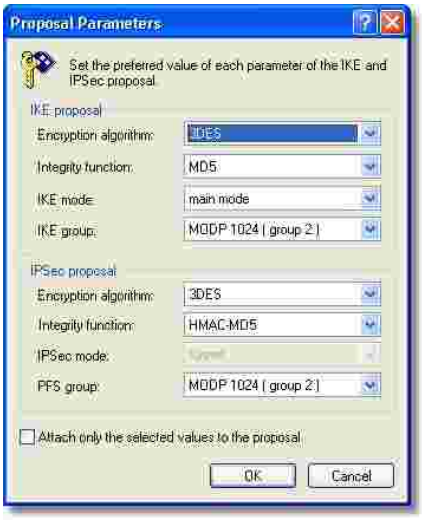
Network Editor

Add VPN connection

In the "Authentication key" field, you should choose the preshared key previously created (myVPNKey). The encryption and authentication settings have to be consistent with those defined when creating the tunnel in edgeBOX, so you should confirm this by selecting "Properties" in the "Add VPN Connection" dialog.

© 2006 Critical Links, SA

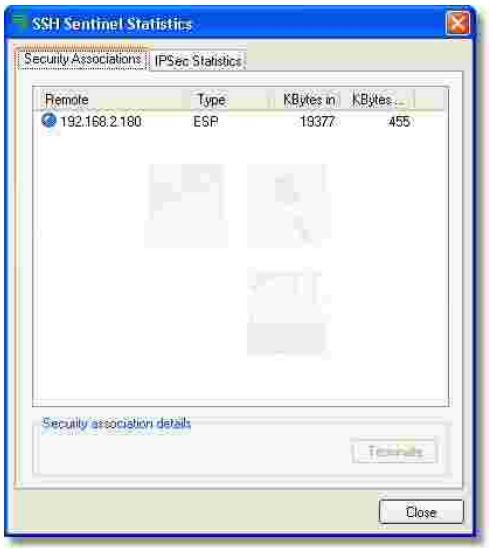
Rule Properties



Proposal Parameters

The "Rule Properties" dialog window will be visible. Under "IPSec/IKE proposal" select "Settings", and make the necessary changes in the dialog window that pops-up (Proposal Parameters) namely, in the encryption algorithm and integrity function.
After confirming all your choices, you should return to the "Policy Editor" window, where the tunnel just created should now be visible under "VPN Connections". To open the connection, select this VPN configuration in the initial menu.

Policy Editor



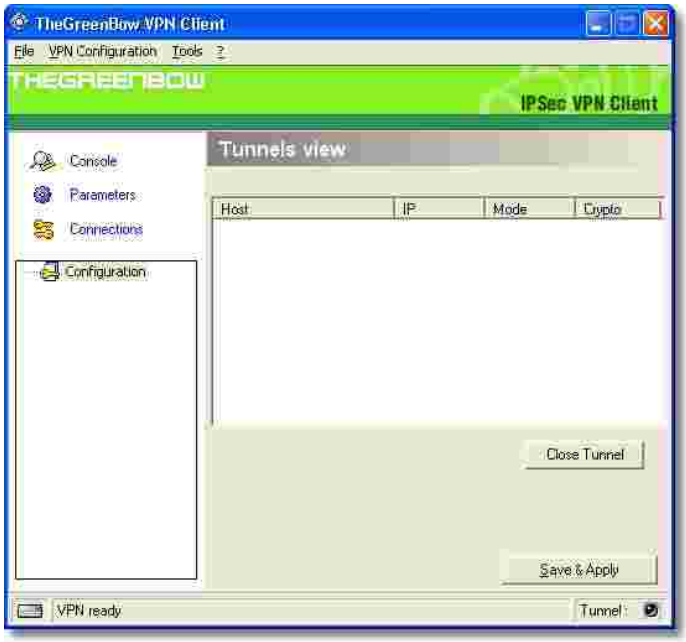
SSH Sentinel Statistics

You can confirm the connection was in fact established checking SSH Sentinel's Statistics window or edgeBOX's VPN panel, where the new opened tunnel will appear under "Active Tunnels".

© 2006 Critical Links, SA

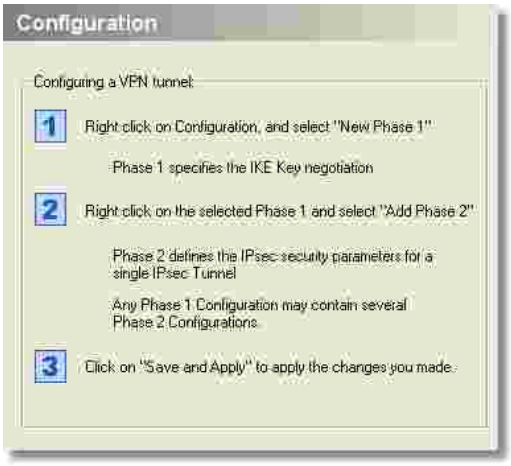
10.1.2 GreenBow

Another certified IPsec VPN client is the GreenBow VPN client. After installation, an icon will be visible in the tray bar. Selecting this icon will display the following window:

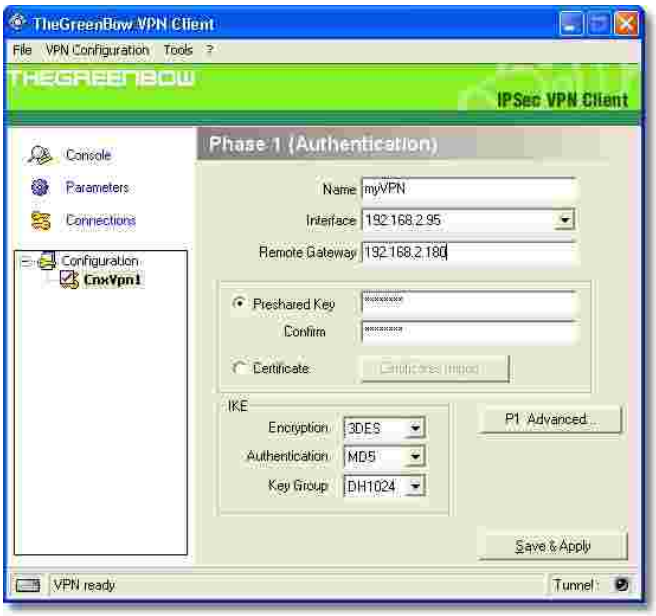


Selecting "Configuration" will display the following information on the panel on the right.

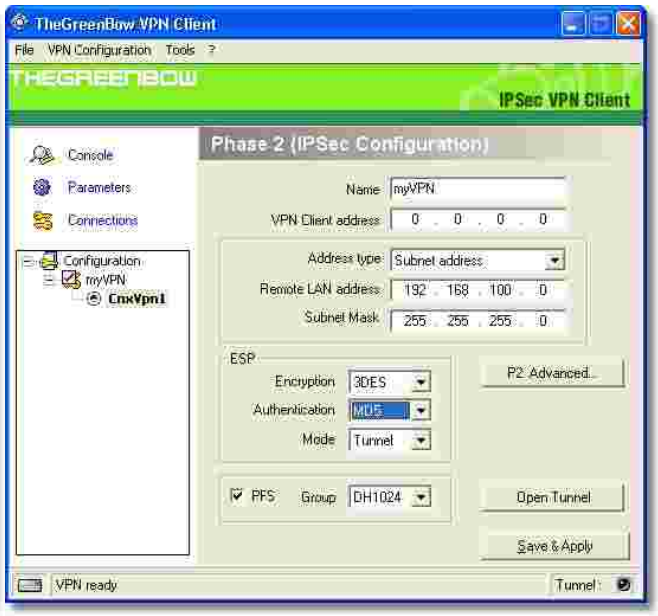
© 2006 Critical Links, SA


Configuration
Configuring a VPN tunnel
1
Right click on Configuration, and select "New Phase 1"
Phase 1 specifies the IKE Key negotiation
2
Right click on the selected Phase 1 and select "Add Phase 2"
Phase 2 defines the IPsec security parameters for a single IPsec Tunnel
Any Phase 1 Configuration may contain several Phase 2 Configurations
3
Click on "Save and Apply" to apply the changes you made

VPN tunnel configuration is done in two steps. To start phase 1 right-click on "Configuration" and select "New Phase 1". The following window will be then visible. Remember that the security settings must be consistent with the settings entered when the tunnel was created on edgeBOX. Change the remaining parameters to fit your situation (in our example, 192.168.2.180 is edgeBOX's external interface and 192.168.2.95 is the client's IP address of the interface to be used). After pressing "Saving & Apply", right-click "myVPN" and select "Add Phase 2".



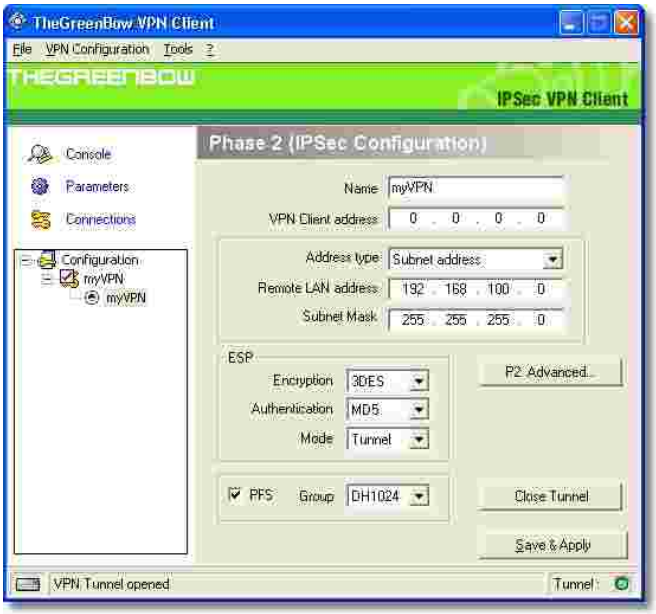
Phase 1



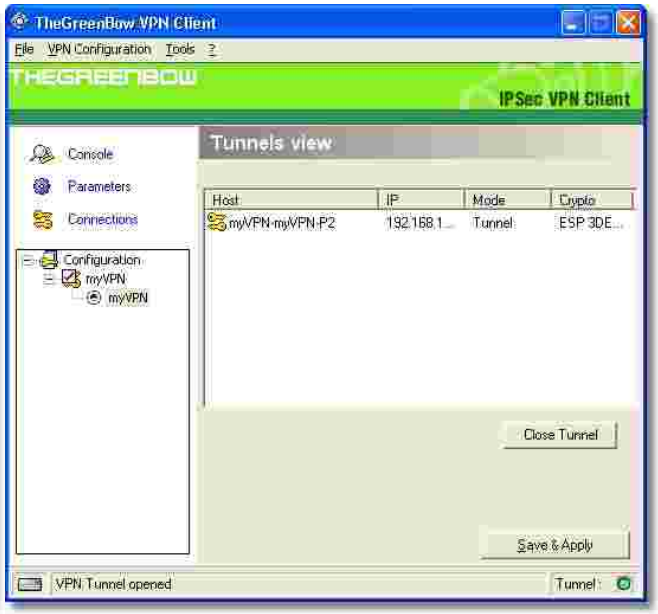
Phase 2

In phase 2, for a RoadWarrior configuration, select 0.0.0.0 as your VPN client address. To access edgeBOX's LAN, select "Subnet address" in "Address type", and fill in the data for "Remote LAN address" and "Subnet Mask" (we used edgeBOX's default settings - 192.168.100.0/24). Don't forget to check if the encryption and authentication schemes used are consistent with those configured in edgeBOX. After entering all the required information press "Save & Apply".

© 2006 Critical Links, SA

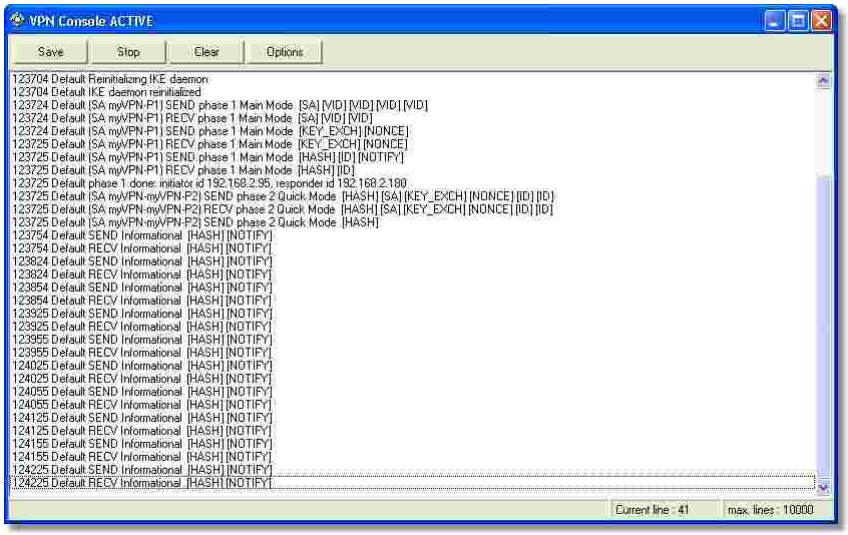


Tunnel opened



Connections

You will then be able to establish the connection selecting the "Open Tunnel" button. If the tunnel was successfully opened, the sentence "VPN Tunnel opened" will be displayed in the status bar, as well as a green light. You can check all connections active selecting "Connections", and check all messages exchanged during connection establishment selecting "Console".

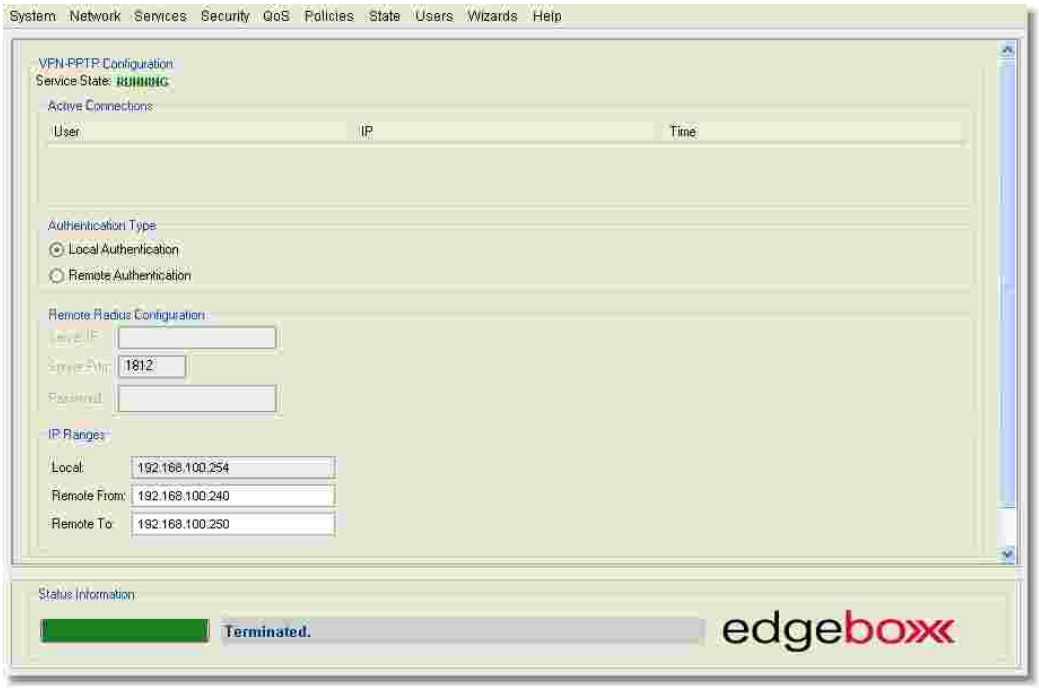

VPN Console ACTIVE
Save
Stop
Clear
Options
123704 Default Reinitializing IKE daemon
123704 Default IKE daemon reinitialized
123724 Default (SA myVPN-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID]
123724 Default (SA myVPN-P1) RECV phase 1 Main Mode [SA] [VID] [VID]
123724 Default (SA myVPN-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE]
123725 Default (SA myVPN-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE]
123725 Default (SA myVPN-P1) SEND phase 1 Main Mode [HASH] [ID] [NOTIFY]
123725 Default (SA myVPN-P1) RECV phase 1 Main Mode [HASH] [ID]
123725 Default phase 1 done: initiator id 192.168.2.95, responder id 192.168.2.180
123725 Default (SA myVPN-myVPN-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
123725 Default (SA myVPN-myVPN-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
123725 Default (SA myVPN-myVPN-P2) SEND phase 2 Quick Mode [HASH]
123754 Default SEND Informational [HASH] [NOTIFY]
123754 Default RECV Informational [HASH] [NOTIFY]
123824 Default SEND Informational [HASH] [NOTIFY]
123824 Default RECV Informational [HASH] [NOTIFY]
123854 Default SEND Informational [HASH] [NOTIFY]
123854 Default RECV Informational [HASH] [NOTIFY]
123925 Default SEND Informational [HASH] [NOTIFY]
123925 Default RECV Informational [HASH] [NOTIFY]
123955 Default SEND Informational [HASH] [NOTIFY]
123955 Default RECV Informational [HASH] [NOTIFY]
124025 Default SEND Informational [HASH] [NOTIFY]
124025 Default RECV Informational [HASH] [NOTIFY]
124055 Default SEND Informational [HASH] [NOTIFY]
124055 Default RECV Informational [HASH] [NOTIFY]
124125 Default SEND Informational [HASH] [NOTIFY]
124125 Default RECV Informational [HASH] [NOTIFY]
124155 Default SEND Informational [HASH] [NOTIFY]
124155 Default RECV Informational [HASH] [NOTIFY]
124225 Default SEND Informational [HASH] [NOTIFY]
124225 Default RECV Informational [HASH] [NOTIFY]
Current line : 41
max. lines : 10000

console

10.2 PPTP VPNs

Next, it will be shown how to setup a PPTP VPN connection to edgeBOX using Microsoft Windows' PPTP client.
edgeBOX setup just requires the PPTP service to be started, and an user authorised to use PPTP VPNs to exist.

© 2006 Critical Links, SA



Microsoft Windows' "New Connection Wizard" will be used to create a PPTP connection.

10.2.1 New connection wizard

After selecting the "New Connection Wizard", an initial welcome window will be shown. Select "Next" to proceed to the "Network Connection Type". In this window, select "Connect to the network at my workplace", and then press "Next".
The "Network Connection" dialog window will be shown, where you should choose the "Virtual Private Network connection" option, and press "Next".

© 2006 Critical Links, SA

New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
Connect to the Internet.
Connect to a private network, such as your workplace network.
To continue, click Next.
< Back
Next >
Cancel

Initial dialog

New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

Network Connection Type

New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >

Network Connection

In the next step, you will be required to enter a name to identify your PPTP connection. Press "Next" to proceed to the "Public Network" window, and choose the option best suited to your situation. After you press "Next", the "VPN Server Selection" window will be shown. Here, you will be required to enter the host name or IP address of your edgeBOX. This will be the external IP address. After you do this, select "Next" to proceed to the next step.

New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
VPN
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel

Connection Name

New Connection Wizard
Public Network
Windows can make sure the public network is connected first.
Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.
Do not dial the initial connection
Automatically dial this initial connection:
< Back
Next >
Cancel

Public Network

New Connection Wizard
VPN Server Selection
What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1):
192.168.2.180
< Back
Next >

VPN Server Selection

The "Connection Availability" dialog window will then be shown. Select the option that best fits your case. After pressing "Next", the final dialog will be shown. After pressing the "Finish" button, the connection dialog will be shown. Before establishing the connection, you should change some of its properties. To do that, select "Properties".

New Connection Wizard
Connection Availability
You can make the new connection available to any user or only to yourself.
A connection that is created for your use only is saved in your user account and is not available unless you are logged on.
Create this connection for:
Anyone's use
My use only
< Back
Next >
Cancel

Connection Availability

New Connection Wizard
Completing the New Connection Wizard
You have successfully completed the steps needed to create the following connection:
VPN
The connection will be saved in the Network Connections folder.
Add a shortcut to this connection to my desktop
To create the connection and close this wizard, click Finish.
< Back
Finish
Cancel

Final dialog

© 2006 Critical Links, SA

connection dialog

10.2.2 Editing the PPTP connection properties

Select the "Networking" tab and choose "PPTP VPN" in "Type of VPN".

After that, select "Internet Protocol (TCP/IP). In the window that pops-up, select "Advanced". Uncheck the "Use default gateway on remote network", and confirm until you see the dialing window. You will then be ready to establish the PPTP VPN connection.

© 2006 Critical Links, SA

Advanced TCP/IP Settings
General
DNS
WINS
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.
Use default gateway on remote network
OK
Cancel

10.2.3 Connecting to edgeBOX

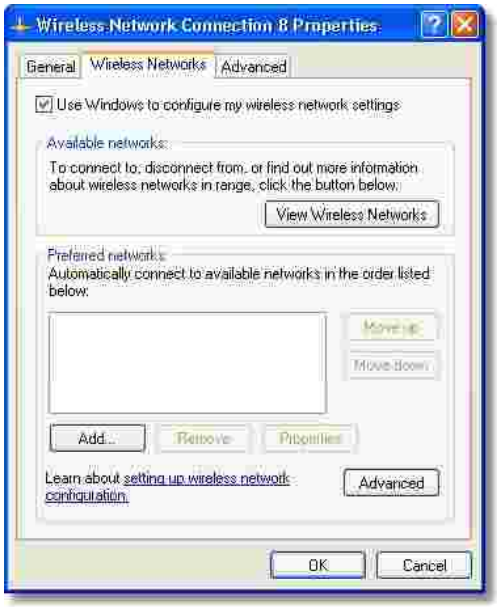
To connect to edgeBOX's PPTP VPN server just enter the user's credentials and select "Connect".

After the connection is successfully established (a small hint will be displayed near the tray bar), the PPTP panel in edgeBOX's control centre will display its information.

© 2006 Critical Links, SA

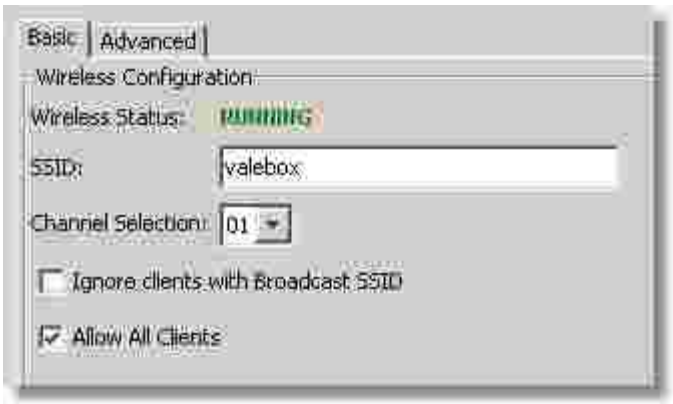
11 Appendix C: Connecting to Wireless

In this appendix it will be shown how to configure a MS Windows client station to connect to edgeBOX's wireless access point using 802.1x and WPA.
Not all wireless cards will support these security schemes - a firmware upgrade may be needed in some cases. Some cards have their own managing software. In the examples that follow, only the native MS Windows client was used. To be able to have MS Windows controlling your Wireless connection, you must start the "Wireless Zero Configuration" service.



Wireless configuration applet.
Notice that windows is being used to configure wireless

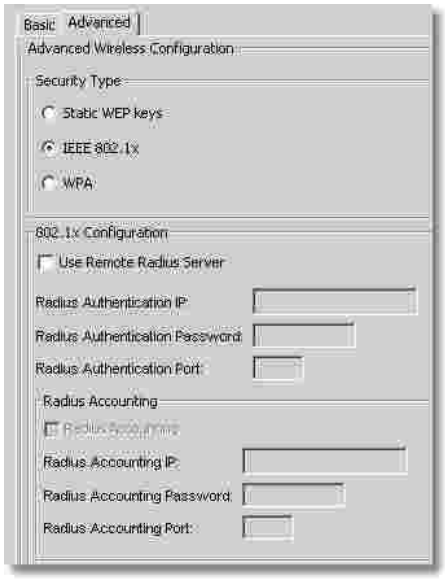
In the examples that follow, the following general configuration will be used:



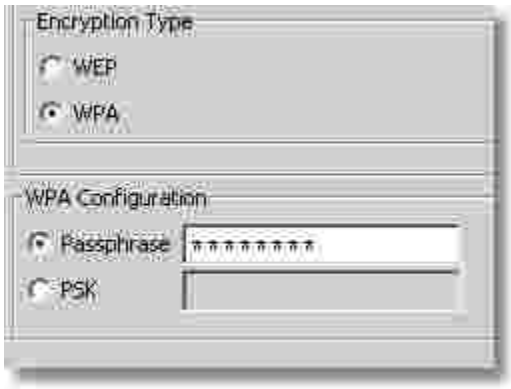
11.1 802.1x

Remember that in order to use 802.1x, you need to authorise "Wireless Security" on the user management.
The following pictures illustrate the configuration used on edgeBOX.

© 2006 Critical Links, SA



security type: 802.1x



encryption type: WPA

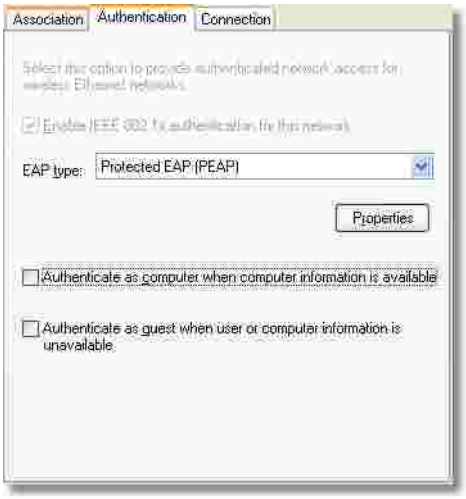
On MS Windows, double-click the "Wireless Network Connection" icon and select the "Wireless Networks" tab. Make sure the SSID entered is consistent with that defined on edgeBOX (valebox on our example). Choose "WPA" for "Network Authentication" and "AES" for "Data Encryption". Select then the "Authentication" tab.

Wireless Network Connection

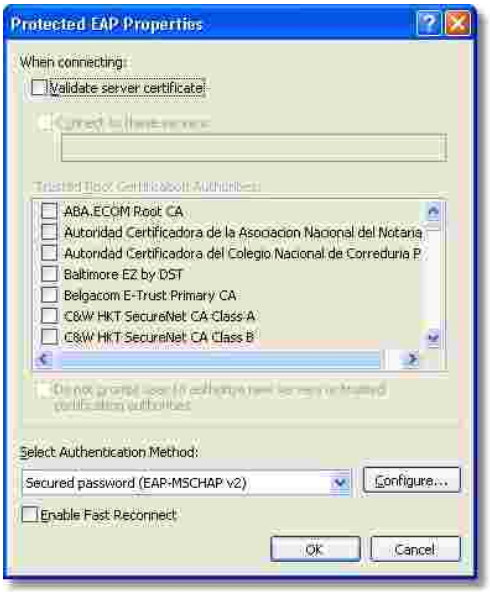
Wireless Networks

On the Authentication tab, select "Protected EAP (PEAP)" as the "EAP type". Press the "Properties" button. On the dialog window that pops-up, uncheck the "Validate server certificate" checkbox, and select "Secure password" as the Authentication Method. Press the "Configure" button.

© 2006 Critical Links, SA



Authentication



Protected EAP Properties

On the dialog window that pops-up, uncheck the "Automatically use my Windows..." checkbox. Press "OK" on all dialogs to confirm this configuration.

If the configuration succeeds, you should see a balloon warning you to enter credentials to connect to the wireless network. Clicking on the balloon will display a prompt requiring you to enter the username and password for a user authorised to connect to the Wireless network.

Wireless Network Connection 8
Click here to select a certificate or other credentials for connection to the network valebox

If the connection was successful, its status will appear as "Connected".

© 2006 Critical Links, SA

Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
valebox
Connected
Security-enabled wireless network (WPA)

11.2 WPA

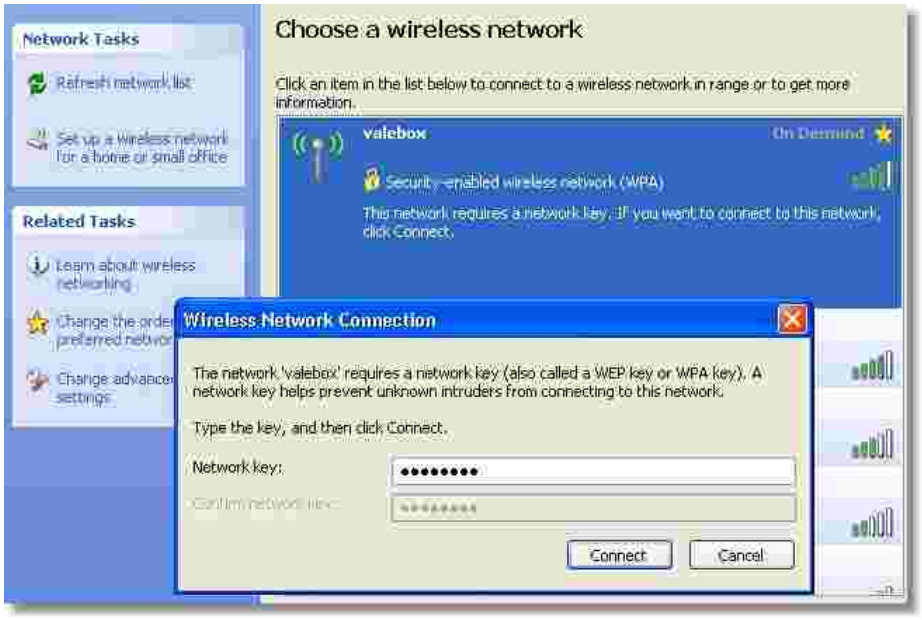
If edgeBOX was configured to use WPA as the security scheme, the following settings must be configured on the client:

- Network Authentication: WPA-PSK
- Data Encryption: AES.

Additionally, the network key to be used must also be supplied. Remember that if you choose to use a preshared key, it must have exactly 64 hexadecimal characters. If this connection is configured to be established manually, when you try to connect to it a dialog window will be shown, asking you to supply the network key.

Wireless Configuration

© 2006 Critical Links, SA


Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
valebox
On Demand
Security-enabled wireless network (WPA)
This network requires a network key. If you want to connect to this network, click Connect.
Wireless Network Connection
The network 'valebox' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.
Type the key, and then click Connect.
Network key:
Connect
Cancel

Network key dialog

© 2006 Critical Links, SA

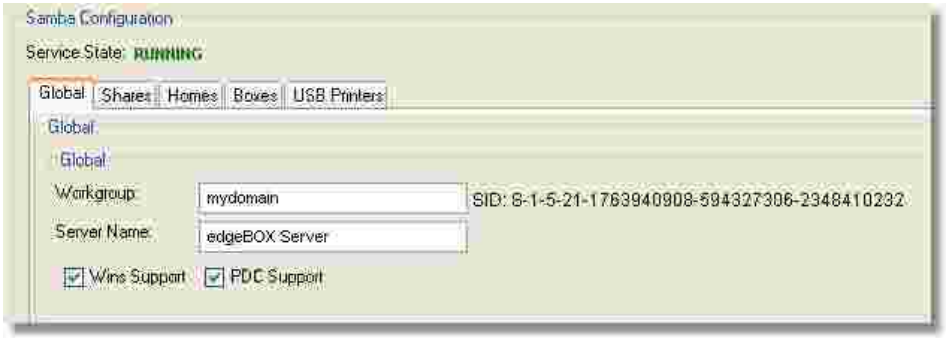
12 Appendix D: Using Samba

In this appendix it will be shown how to use some of Samba's features, namely how to use edgeBOX as a PDC and how to use the safes' functionality. Remember that users must be authorised to use "Windows use" upon their creation in the system.

user creation dialog

12.1 edgeBOX as a PDC

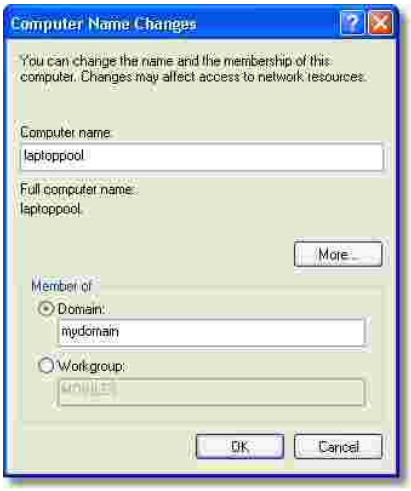
To configure edgeBOX to work as a PDC all it has to be done is to check the "PDC Support" option on the Samba panel.



edgeBOX configured as PDC for mydomain

To add a machine to edgeBOX's domain, select "System" under the Windows Control Panel, and then select the "Computer Name" tab. Select the "Change" button. In the dialog window that pops-up, select the "Domain" option and enter your domain name (in our example it was "mydomain"). After you select "OK" to confirm the domain change, you will be required to supply credentials of a user belonging to the domain administrator's group. In edgeBOX, you have to specifically supply the username "Administrator", which has the same password as the admin user (defaults to root).

© 2006 Critical Links, SA

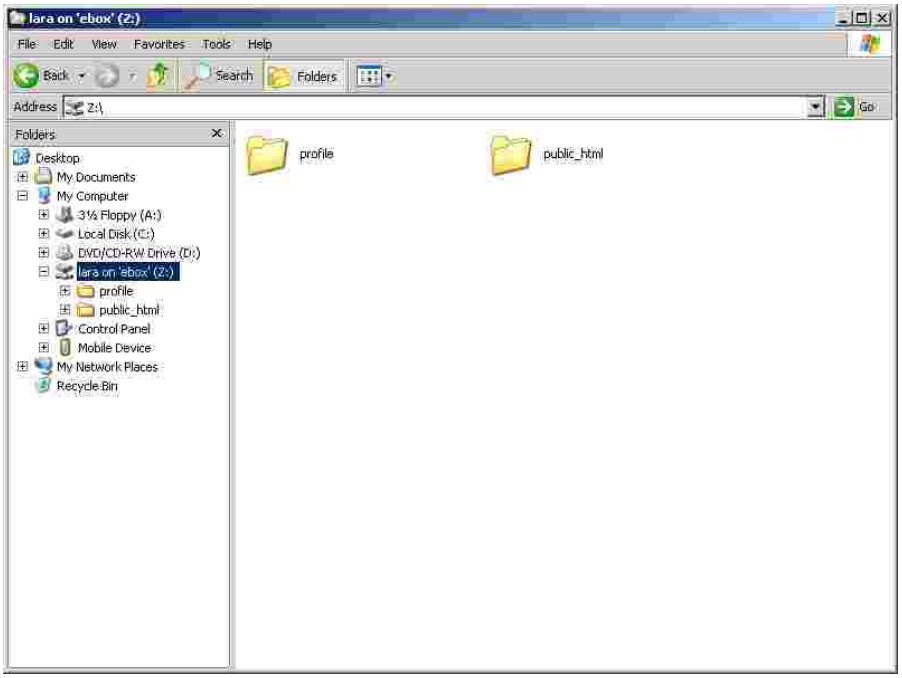


change domain dialog

join domain dialog

If the operations was successful, the following dialog will be displayed.

After rebooting the machine, log on to edgeBOX's domain (it should be available on the domains' list). The user's home directory will be mounted as Z:. In the picture bellow the user's directory content is shown, where the public_html directory can be accessed. This is the directory where the user's personal web page will be located. The other directory shown (profile) is where the roaming profile data will be stored, so the user will retain her desktop definitions after logging off.



© 2006 Critical Links, SA

12.2 Public safes

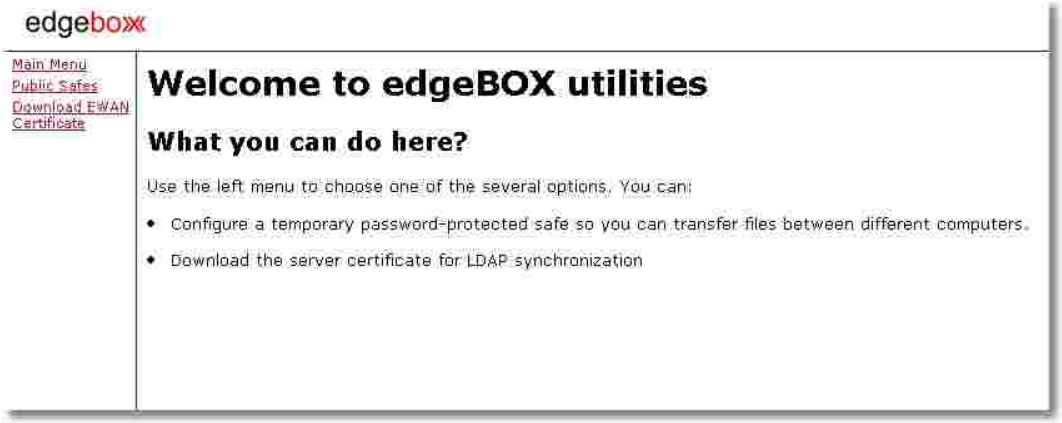
Safes are available only for LAN users and may be used when there's a need for a temporary space for storage. Any user on your network can ask for a box to store files and access it as a normal Windows share. To be able to use safes, the following conditions must be met:

- The Samba service must be started;
- Boxes must be active;
- The user must be authorised to use Samba.

The options available for configuration are the maximum size of safes, their maximum availability and the maximum number of safes active at the same time.

Configuration options for safes

Any LAN user can request a safe accessing the utilities page (http://<lan address>:8010 and following the "Services" option). The following page will be displayed.


edgeboxx
Main Menu
Public Safes
Download EWAN Certificate
Welcome to edgeBOX utilities
What you can do here?
Use the left menu to choose one of the several options. You can:
Configure a temporary password-protected safe so you can transfer files between different computers.
Download the server certificate for LDAP synchronization

edgeBOX utilities entry page

Follow the link "Public Safes". Currently available safes will be displayed, as well as the current safes' configuration parameters. To create a new safe, select "Create a new safe".

© 2006 Critical Links, SA

Public Safes

Select the desired settings for your safe. Sizes available will always be less than or equal to the maximum size configured, as well as the maximum time the safe will be available. To create the safe, select "Create safe".

Safe creation window

If the safe was successfully created, credentials to access it will be displayed.

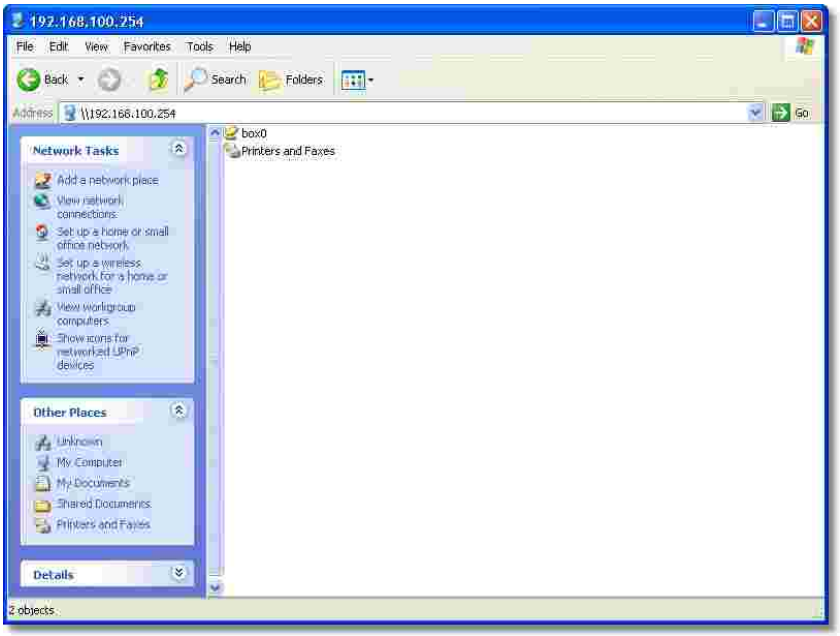
credentials to access the safe

Selecting "Public Safes" again will now display the safe just created.

© 2006 Critical Links, SA

Public safes list

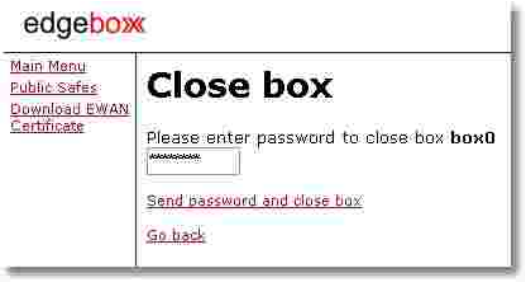
To use the safe, access it like a normal windows share, entering the credentials supplied to authenticate.



If you want to close the safe before its time expires, go to the utilities' menu and follow the "Close

© 2006 Critical Links, SA

this box" link next to the safe you want to close. You will need to supply the password for the safe. If the operation completes successfully, the message "Box closed" will be displayed.



© 2006 Critical Links, SA

13 Appendix E: Virtual Hosts

You can host several websites in edgeBOX and access them using different hostnames. The HTTP server will fetch the correct website requested. This is the web server's virtual hosts feature. Next is a description on how to create virtual hosts.

Suppose you want to have an internal domain local.loc, and want to have two websites: www.local.loc (the main website, for example a company's website) and a departmental website, for example marketing.local.loc. To have this configuration, you should perform the following steps:

- Create DNS hosts for the websites you want to create. In this case, if the internal IP of edgeBOX is 192.168.100.254, you will have to create A records in DNS, pointing to this address for www and marketing. For information on creating records on DNS, check Hosts.

Next, you will need to upload files for your websites. For clarity, you can create two separate directory trees for your websites. The steps to do this are:

- In control centre under the HTTP panel change the webmaster's password if you haven't done so yet;
- Connect to edgeBOX's FTP server with the webmaster username. Create a directory to host the marketing website files (for example, at the same level as inter, the directory for the main website);
- Upload the files for you websites;

For the virtual hosts' configuration, under the HTTP panel select New in the virtual hosts section to create a new virtual host. In the window that pops-up, insert the following:

- Virtual Host: LAN (in this case, we are configuring a LAN-only accessible virtual host);
- Server Name: marketing;
- Document Root: change to "path" and insert "marketing" (the name of the directory created - this is a relative path to the web site's root);
- Email: the email for the webmaster responsible for this website. It is not a mandatory field.

After applying this information, you will be able to access marketing.local.loc. However, the main website will not probably be available and so, you will need to create another virtual host, this time for your main web site. Select "New" again, to add a virtual host and enter the following data:

- Virtual Host: LAN;
- Server Name: www;
- Document Root: inter.

After applying this information, you should be able to access your main site using http://www.local.loc, and the marketing website using http://marketing.local.loc.

© 2006 Critical Links, SA

14 Appendix F: Softphone configuration

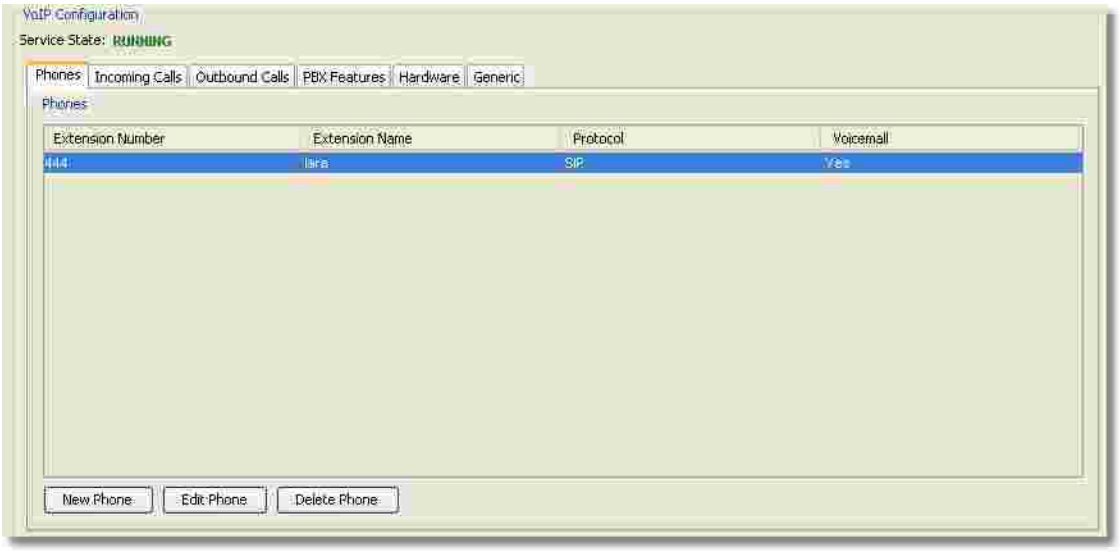
Next, it will be shown how to configure three different softphones. There is a wide variety of softphones available. The following will be shown:

- X-Lite
- Idefisk
- Express Talk.

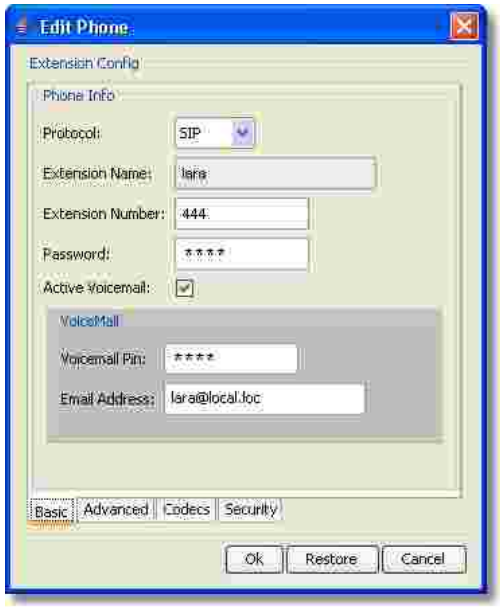
First, on the edgeBOX side, a phone must be added to the system. That happens automatically upon user creation when access to the VoIP service is granted.

The extension name will have the same name as the user's username.

© 2006 Critical Links, SA



When connecting behind a gateway remember to use "Nat" under "Advanced".



14.1 X-Lite

X-Lite is a SIP softphone. It can be downloaded from http://www.xten.com/index.php?menu=download.
Installation and basic configuration (such as audio) are out of the scope of this text. Next, the connection configuration options are displayed.

© 2006 Critical Links, SA

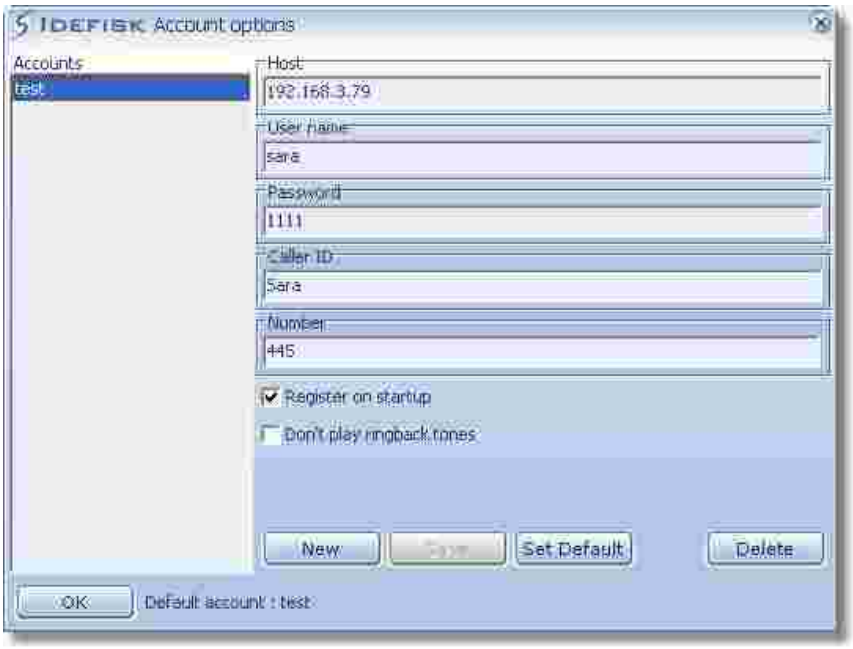
Selecting 'back' until the root menu is reached, and then expanding the "Network" options, change the "Out Bound SIP Proxy".
The softphone is now configured and should be able to register in the edgeBOX.

You can then dial 9999 to test your connection.

© 2006 Critical Links, SA

14.2 Idefisk

Idefisk is an IAX2 softphone which can be downloaded from http://www.asteriskguru.com/tools/idefisk_beta.php.
Next, the connection configuration options are displayed.

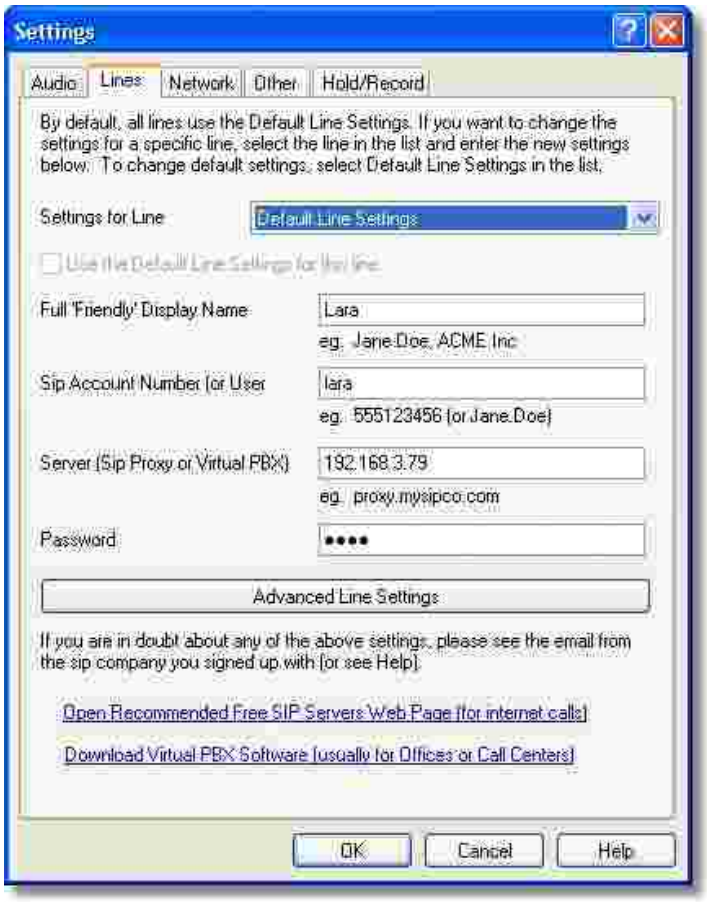


Again the number 9999 can be dialed to test if the connection is working properly.

© 2006 Critical Links, SA

14.3 Express Talk

Express Talk is a SIP softphone, which can be downloaded from http://www.nch.com.au/talk/index.html.
Next, the connection configuration options are shown:


Settings
Audio
Lines
Network
Other
Hold/Record
By default, all lines use the Default Line Settings. If you want to change the settings for a specific line, select the line in the list and enter the new settings below. To change default settings, select Default Line Settings in the list.
Settings for Line
Default Line Settings
Full 'Friendly' Display Name
Lara
eg. Jane Doe, ACME Inc
Sip Account Number (or User
lara
eg. 555123456 (or Jane.Doe)
Server (Sip Proxy or Virtual PBX)
192.168.3.79
eg. proxy.mysipco.com
Password
Advanced Line Settings
If you are in doubt about any of the above settings, please see the email from the sip company you signed up with (or see Help).
Open Recommended Free SIP Servers Web Page (for internet calls)
Download Virtual PBX Software (usually for Offices or Call Centers)
OK
Cancel
Help

The dial window has a log panel where call details can be checked. Again, the number 9999 has been dialed to confirm registration success.

© 2006 Critical Links, SA

Express Talk
Talk View Help
Address Logs Invite Settings Help
1 ABC 2 DEF 3
GHI 4 JKL 5 MNO 6
PQRS 7 TUV 8 WXYZ 9
DEL * 0 ENTER #
Hold
Transfer
Record
Do Not Disturb
18:12:48 Call has disconnected
18:12:48 Initiated sip call to: 9999
18:12:48 Unable to auto-detect public IP. Using private IP
18:12:48 Call answered
18:13:03 Call has disconnected
18:13:08 Initiated sip call to: 999
18:13:08 Unable to auto-detect public IP. Using private IP
18:13:08 Call answered
18:13:16 Call has disconnected
For more audio software www.nch.com.au/software

© 2006 Critical Links, SA

15 END USER LICENSE AGREEMENT (EULA)

END-USER LICENSE AGREEMENT (EULA)

FOR Critical Software S.A. (CRITICAL)
EDGEBOX Software

October 2005

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Critical Software S.A. (hereinafter "CRITICAL"), the manufacturer, for use of the Edgebox (tm) software ("Licensed Software"). By installing, copying or otherwise using the Licensed Software, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, CRITICAL is unwilling to license the software to you. In such event, you may not use or copy the Licensed Software.

1. Definitions

1.1. "CRITICAL" shall mean Critical Software S.A. and any of its affiliates such as Critical Software Inc and Critical Software technologies Ltd..

1.2. "Licensed Software" shall mean the EdgeBox software. The term Licensed Software is understood to specially include any and all Licensed Software Documentation but specifically does not include open-source components. Please see Section 8 for details on open-source components.

1.3. The Licensed Software is intended for use in a single Computer..

1.4. “License keys” shall mean activation codes provided directly by Critical or its partners that are used by licensed users of the EdgeBox Software to activate its functionality for an authorized Computer. An authorized Computer is identified by a signature build of hardware parts unique serial numbers or alternatively, a USB dongle.

2. Ownership

The foregoing license gives you limited license to use the Software. CRITICAL retain all right, title and interest, including all copyright and intellectual property rights, in and to, the Licensed Software and all copies thereof. All rights not specifically granted in this EULA, including Federal and International Copyrights, are reserved by CRITICAL.

3. License Grants

3.1. If the Licensed Software is in use on a certain Computer, you may not use or copy the Licensed Software to additional Computers except where provisions within this agreement have been made.

3.2. The software is activated by a license key provided by CRITICAL at the time of purchase. Please refer to the license details in the User Manual provided to you by Critical Software.

3.3. The Licensed Software is designed to function only within Computer models that are qualified by Critical. Please see EdgeBox web page for more details. Attempts to use the

© 2006 Critical Links, SA

Licensed Software on other computers are in violation of the EULA.

3.4. You may use software back-up utilities to make a back-up copy of the Licensed Software. You may use the back-up copy solely for archival purposes.

3.5. Your license rights under this EULA are non-exclusive.

3.6. Certain rights are not granted under this Agreement, but may be available under a separate agreement. If you would like to enter into a Distribution or OEM Agreement, please contact Critical Software S.A.

3.7. This license does not entitles the user to any maintenance and technical support for the Licensed Software provided by CRITICAL or its Partner's. Annual Maintenance and Support may be purchased separately from CRITICAL or its Partners. Please contact CRITICAL for more information.

4. License Restrictions

4.1. You may not reverse engineer, decompile, or disassemble the Licensed Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

4.2. You may not sell, rent, lease, or sublicense the Licensed Software.

4.3. You may not modify the Software or create derivative works based upon the Software.

4.4. The Licensed Software is licensed as a single product. Its component parts may not be separated for use beyond the the authorized Computer.

4.5. You may permanently transfer all of your rights under this EULA only as part of a sale or transfer of the Computer, provided you retain no copies, you transfer all of the Licensed Software (including all component parts, the media and printed materials, any upgrades, this EULA and, if applicable, the Certificate(s) of Authenticity), AND the recipient agrees to the terms of this EULA. If the Licensed Software is an upgrade, any transfer must include all prior versions of the Licensed Software. For value added support, notification of CRITICAL of the transfer is strongly recommended.

4.6. In the event that you fail to comply with this EULA, CRITICAL may immediately terminate the license and you must destroy all copies of the Software (with all other rights of both parties and all other provisions of this EULA surviving any such termination).

5. Limited Software Warranty

5.1. CRITICAL warrants that the Licensed Software will function substantially in accordance with the documentation and specification for its operation, for a period of 30 (thirty) days and will work on a best effort basis to correct flaws. However, the Licensed Software is licensed without any warranty of merchantability or fitness for any particular purpose.

5.2. CRITICAL shall not be responsible for any consequential or any other direct or indirect damages arising from the use of the Licensed Software or related components or documentation, even if it has been advised of the possibility of such damages.

5.3. No oral or written information or advice given by CRITICAL, its dealers, distributors, agents or employees shall create a warranty or in any way increase the scope of any warranty provided herein.

© 2006 Critical Links, SA

5.4. You may have other rights, and these rights as a consumer may vary from country to country.

6. Upgrades

If the Licensed Software is an upgrade from another product, whether or not from CRITICAL you may use or transfer the Licensed Software only in conjunction with that upgraded product, unless you destroy the upgraded product. If the Licensed Software is an upgrade of a CRITICAL product, you now may use that upgraded product only in accordance with this EULA. .

7. General

7.1. This EULA shall be governed by the laws of Portugal, without giving effect to principles of conflict of laws. You hereby consent to the exclusive jurisdiction and venue of the courts sitting in Lisbon, Portugal to resolve any disputes arising under this EULA.

7.2. This EULA contains the complete agreement between the parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous agreements or understandings, whether oral or written. You agree that any varying or additional terms contained in any purchase order or other written notification or document issued by you in relation to the Software licensed hereunder shall be of no effect. The failure or delay of CRITICAL to exercise any of its rights under this EULA or upon any breach of this EULA shall not be deemed a waiver of those rights or of the breach.

7.3. No CRITICAL dealer, agent or employee is authorized to make any amendment to this EULA.

7.4. If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, that provision will be enforced to the maximum extent permissible, and the remaining provisions of this Agreement will remain in full force and effect.

7.5. All questions concerning this EULA shall be directed to: Critical Software S.A., Parque Industrial de Taveiro, Lote 48, 3045-504 Coimbra, Portugal, Attention: General Manager - edgebox.support@critical-links.com

7.6. CRITICAL and other trademarks contained in the Software are trademarks or registered trademarks of Critical Software S.A. Third party trademarks, trade names, product names and logos may be the trademarks or registered trademarks of their respective owners. You may not remove or alter any trademark, trade names, product names, logo, copyright or other proprietary notices, legends, symbols or labels in the Software. This EULA does not authorize you to use Critical's or its licensors' names or any of their respective trademarks.

8. Open Source Software Components

5.5. The EdgeBox software is shipped in the same medium as open source software components that are specifically not covered by this EULA.

5.6. This EULA only covers software components that have been developed and are propriety of Critical Software, SA.

5.7. The Open Source software components aggregated in the same medium as EdgeBox Software have their own end user license agreements. Please see Annex A for their respective license text.

Manufacturer of Licensed Software is:

© 2006 Critical Links, SA

Critical Software S.A.
Parque Industrial de Taveiro, Lote 48
3045-504 Coimbra, Portugal
Tel:+351.239989100
Fax:+351.239989119
http://www.criticalsoftware.com
http://www.edgebox.net
edgebox.support@critical-links.com

© 2006 Critical Links, SA

© 2006 Critical Links, SA

16 Licence texts

LICENSE TEXTS FOR OPEN-SOURCE COMPONENTS AGRREGATED IN THE SAME MEDIA AS EDGEBOX SOFTWARE

Version 1, March 2005

1. GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source

© 2006 Critical Links, SA

code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.
However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.
You are not responsible for enforcing compliance by third parties to
this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions
of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author
to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software

© 2006 Critical Links, SA

Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2. The OpenLDAP Public License

Version 2.7, 7 September 2001

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

© 2006 Critical Links, SA

3. Apache License

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

4. The PHP License

The PHP License, version 3.0
Copyright (c) 1999 - 2002 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes PHP, freely available from <http://www.php.net/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see <http://www.php.net>.

This product includes the Zend Engine, freely available at <http://www.zend.com>.

5. SENDMAIL LICENSE

The following license terms and conditions apply, unless a different license is obtained from Sendmail, Inc., 6425 Christie Ave, Fourth Floor, Emeryville, CA 94608, USA, or by electronic mail at license@sendmail.com.

License Terms:

© 2006 Critical Links, SA

Use, Modification and Redistribution (including distribution of any modified or derived work) in source and binary forms is permitted only if
each of the following conditions is met:

1. Redistributions qualify as "freeware" or "Open Source Software" under one of the following terms:

    (a) Redistributions are made at no charge beyond the reasonable cost of materials and delivery.

    (b) Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means the complete compilable and linkable source code of sendmail including all modifications.

2. Redistributions of source code must retain the copyright notices as they appear in each source code file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.

3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:
"Copyright (c) 1998-2003 Sendmail, Inc. All rights reserved."

4. Neither the name of Sendmail, Inc. nor the University of California nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission. The name "sendmail" is a trademark of Sendmail, Inc.

5. All redistributions must comply with the conditions imposed by the University of California on certain embedded code, whose copyright notice and conditions for redistribution are as follows:

    (a) Copyright (c) 1988, 1993 The Regents of the University of California. All rights reserved.

    (b) Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

        (i) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

        (ii) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

        (iii) Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

6. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY SENDMAIL, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL SENDMAIL, INC., THE REGENTS OF THE UNIVERSITY OF CALIFORNIA OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

$Revision: 8.11.2.1 $, Last updated $Date: 2003/04/19 14:30:36 $

6. OpenSSL License

Copyright (c) 1998-2003 The OpenSSL Project.
All rights reserved.

© 2006 Critical Links, SA

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project or use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the

following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
   The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

7. Bind

Copyright (C) 1996-2002 Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

$Id: COPYRIGHT,v 1.6.2.2 2002/02/12 06:05:48 marka Exp $

Portions Copyright (C) 1996-2001 Nominum, Inc.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

8. Curl

COPYRIGHT AND PERMISSION NOTICE
Copyright (c) 1996 - 2003, Daniel Stenberg, <daniel@haxx.se>.
All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

© 2006 Critical Links, SA

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not
be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

9. DB

Copyright (c) 1990-2002
Sleepycat Software. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Redistributions in any form must be accompanied by information on how to obtain complete source code for the DB software and any accompanying software that uses the DB software. The source code must either be included in the distribution or be available for no more than the cost of distribution plus a nominal fee, and must be freely redistributable under reasonable conditions. For an executable file, complete source code means the source code for all modules it contains. It does not include source code for modules or files that typically accompany the major components of the operating system on which the executable file runs.

THIS SOFTWARE IS PROVIDED BY SLEEPYCAT SOFTWARE ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED. IN NO EVENT SHALL SLEEPYCAT SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1990, 1993, 1994, 1995
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

© 2006 Critical Links, SA

Copyright (c) 1995, 1996
The President and Fellows of Harvard University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

10. Expat

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper
Copyright (c) 2001, 2002 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

11. BSD

“This product includes software developed by the University of California, Berkeley and its contributors”

12. LGPL

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change

© 2006 Critical Links, SA

in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the
Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials

© 2006 Critical Links, SA

specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

© 2006 Critical Links, SA

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

13. Sun Microsystems, Inc. Binary Code License Agreement

"This product includes code licensed from RSA Security, Inc.", "Some portions licensed from IBM are available at http://oss.software.ibm.com/icu4j/"

14. Licence for libxslt and libxml

Copyright (C) 2001-2002 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,

© 2006 Critical Links, SA

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not
be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

15. Licence for libxslt

Copyright (C) 2001-2002 Thomas Broyer, Charlie Bozeman and Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the authors shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

© 2006 Critical Links, SA